PRIVACY POLICY

AND

NOTICE

Óbuda Uni Venture Capital Private Limited Company

(1034 Budapest, Bécsi út 96/B)

September 1, 2023

INTRODUCTION

Óbuda Uni Venture Capital Private Limited Company (registered office: 1034 Budapest, Bécsi út 96/B, company registration number: 01-10-142341, tax number: 32271557-2-41, registered by the Company Court of Budapest, hereinafter referred to as the "Company" or "Data Controller") as a company founded by Óbuda University (registered office: 1034 Budapest, Bécsi út 96/B, registration number: FI 12904 "University") are committed to protecting the personal data of their clients and third parties in contact with them, including visitors to the website(s) operated by the Data Controller, especially those at https://obudaunivc.com/ ("Website") (hereinafter referred to as "Data Subjects"). Respecting their right to self-determination in connection with data handling is of paramount importance.

The purpose of creating this policy is to ensure that the Data Controller complies with applicable data protection laws and provides proper information to Data Subjects regarding the processing of their personal data. The Data Controller shall act in accordance with this privacy policy (hereinafter referred to as the "Policy"), as well as its other internal regulations and instructions, in all data processing activities.

The General part of this Policy sets forth general rules applicable to all data processing, while the Special part contains specific rules and information pertaining to individual data processing activities. This Policy encompasses the major data processing activities carried out by the Data Controller, but not all Data Subjects will necessarily be subject to all data processing activities listed herein. For each specific data processing, the Data Controller shall provide a brief data processing notice to Data Subjects regarding the details of that particular data processing.

Please be aware that you should read this Policy carefully, as it includes comments providing information about data processing and data protection, thereby offering a comprehensive picture of the Data Controller's practices and the rights of Data Subjects.

In all data processing activities, the Data Controller will handle the personal data recorded by it or provided to it in a confidential manner, in compliance with data protection laws, and as specified in this Policy, ensuring that the legal goal of enabling everyone to have control over their personal data is achieved. Beyond these, the Data Controller will ensure data security during data processing, take the necessary technical and organizational measures, and establish procedural rules within the framework of a separate policy, all of which are necessary to enforce data and confidentiality protection regulations.

While this Policy, although striving for comprehensive regulation, may not necessarily encompass all data processing activities, should the necessity arise for a new data processing that is not covered by this Policy, the Data Controller will inform Data Subjects about the essential circumstances related to that particular data processing through the publication of a separate data processing notice on each occasion.

A current copy of this Policy must be kept at the registered office of the Company, and this Policy and its amendments are also accessible on the website https://obudaunivc.com/privacy-policy/.

This Policy does not apply to the processing of data related to the Company's employees (including job applicants, temporary employees, and those employed through cooperatives).

RELEVANT LEGISLATION

1. 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, and repealing Directive 95/46/EC (General Data Protection Regulation) (hereinafter referred to as "GDPR").
2. Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (hereinafter referred to as "Info Act").
3. Act C of 2000 on Accounting (hereinafter referred to as "Accounting Act").
4. Act CL of 2017 on the Rules of Taxation (hereinafter referred to as "Taxation Act").
5. Act LIII of 2017 on the Prevention and Combating of Money Laundering and Terrorist Financing (hereinafter referred to as "AML Act").
6. Act CVIII of 2001 on Certain Issues of Electronic Commerce Services and Information Society Services (hereinafter referred to as "E-Commerce Act").

PURPOSE OF THE POLICY

The purpose of this Policy is to ensure the practical implementation of the provisions of relevant legislation, particularly the GDPR, by applying and enforcing the rules set forth in this Policy. Within this framework, the Company, through this Policy, as well as other internal regulations, instructions, and established internal procedures:

- Ensures the fundamental rights of Data Subjects relating to the protection of personal data, compliance with data security requirements, and enforcement thereof.

- Regulates the practice of preventing unauthorized access to data and establishes rules to prevent the unlawful alteration of data, unauthorized use of data, and unauthorized disclosure.

- Specifies the precise and secure procedures for handling, processing, using, transmitting, and destroying data, both in paper and electronic form.

- Provides adequate information to Data Subjects regarding the processing of their personal data, their rights, and how to exercise those rights.

1. GENERAL SECTION

1.1. DEFINITIONS

In the application of this Policy:

"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 one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person – in other words, any data that can be used to identify the Data Subject, such as name, address, telephone number, IP address, etc.

"Data Subject": Any natural person who uses the services of the Data Controller or contacts the Data Controller for that purpose, and whose personal data is processed by the Data Controller.

"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 – in other words, any activity related to data, including data collection, data access, data organization, etc.

"Profiling": Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

"Record Keeping System": A structured set of personal data accessible according to specific criteria, whether centralized, decentralized, or distributed on a functional or geographical basis.

"Data Controller": The 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; where the purposes and means of such processing are determined by Union or Member State law, the Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law – in this case, the Company.

"Data Processor": A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the Data Controller; a Data Processor can be any person or entity that performs specific operations on personal data as instructed by the Company (e.g., accountant/payroll processor, hosting provider, software provider, email service provider, etc.).

"Recipient": A natural or legal person, public authority, agency, or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities

which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules – a recipient is anyone or any authority who receives or has access to the data, e.g., tax authority, data processor, etc.

"Cookie": A file (data record) created by the display program of the Website on the visitor's computer, which stores information about the visitor's connection to the website. The purpose of using cookies is to identify (recognize) the visitor's computer, provide easier browsing, track visits to the Website, analyse and evaluate the usage habits of Website visitors, and improve the user experience. Through cookies placed on the visitor's computer, the start and end times of the user's visit, IP address, and in some cases – depending on the settings of the user's computer – the type of browser, operating system, language, the user's device parameters, settings provided by the user on the Website, visited subpages, and time spent on them can be automatically recorded.

"Third Party": Any natural or legal person, public authority, agency, or other body that is not the Data Subject, the Data Controller, the Data Processor, or persons who, under the direct authority of the Data Controller or the Data Processor, are authorized to process personal data; in general, entities not directly related to data processing are considered third parties.

"Consent of the Data Subject": The voluntary, specific, informed, and unambiguous expression of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; it may include written consent, checking the consent checkbox on the website, etc. It is important to note that, from a data protection perspective, silence cannot be considered as consent.

"**Joint Controller**": where the purposes and means of processing are determined jointly by two or more controllers, they are considered joint controllers and the Data Subject must be informed on this separately.

1.2. PRINCIPLES OF DATA PROCESSING

• **Lawfulness, Fairness, and Transparency** - Personal data must be processed lawfully, fairly, and in a transparent manner for the Data Subject - meaning that data may only be processed in accordance with applicable legal provisions, and the Data Subject should be adequately informed about the circumstances of the data processing (such as purposes, legal basis, duration, etc.).

• **Purpose Limitation** - The collection of personal data must only occur for specified, explicit, and legitimate purposes, and it must not be further processed in a manner incompatible with those purposes (further data processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes is allowed) - which means that data collected for a specific purpose can only exceptionally be used for other purposes.

• **Data Minimization** - The collection of personal data must be adequate, relevant, and limited to what is necessary for the purposes of processing - meaning that personal data may only be processed if there is no other way to achieve the specified purpose.

• **Accuracy** - The collected data must be accurate and kept up to date when necessary; every reasonable step must be taken to ensure that inaccurate personal data is rectified or erased without delay for the purposes of processing - which means that changes in the data must be reflected as soon as possible.

• **Integrity and Confidentiality** - Data processing must be carried out in a manner that ensures the appropriate security of personal data, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage, using appropriate technical or organizational measures - adequate IT and other security measures are necessary to prevent unauthorized access to the data.

• **Storage Limitation** - Personal data must be stored in a form that permits identification of Data Subjects for no longer than is necessary for the purposes of processing; this means that after achieving the specified purpose (maximum processing duration), the data must either be deleted or anonymized so that the Data Subject can no longer be identified from the data.

• **Accountability** - The Data Controller is responsible for compliance with the above principles and must be able to demonstrate such compliance - the Data Controller records its data processing activities through internal instructions and regulations to ensure that processes within the organization are traceable (and can be demonstrated to authorities if necessary).

1.3. PURPOSES AND LEGAL BASES OF DATA PROCESSING

Purposes of Data Processing

The specific purposes of data processing are determined separately for each instance by the Company and are recorded in the Specific Section. In general, the Company processes the data of Data Subjects for the purposes of its operations, the enforcement of contractual rights and obligations arising from contracts, and the protection of legitimate interests.

Legal Bases of Data Processing

Similarly, the legal basis for data processing is determined separately by the Company for each instance and is also recorded in the Specific Section.

The GDPR distinguishes six types of legal bases for data processing, which are as follows:

• Consent-Based Data Processing (Consent of the Data Subject)

Consent from the Data Subject is always voluntary and can only be given through some form of active action (silence or inaction does not constitute consent). Examples of consent include written consent (either in a separate statement or, for example, by signing a contract that contains consent), clicking a checkbox on an electronic interface, or clicking an "I agree" button, etc.

The Data Subject has the right to withdraw consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal, meaning that consent can only be withdrawn for future processing.

Withdrawal of consent can be made in writing, by phone, or in the form of a statement sent by email.

In the case of a person under 16 years of age or a person with limited legal capacity, the consent of the parent exercising parental rights or the guardian is required for processing the data of an individual under 16 years of age.

In case of doubt, it must be presumed that the Data Subject did not give consent.

• Data Processing Necessary for the Conclusion or Performance of a Contract in which the Data Subject is a Party (Contractual Obligation)

If processing of personal data is necessary for the performance of a contract and the Data Subject is a party to the contract, this can serve as a lawful basis for processing. In such cases, separate consent from the Data Subject is not required. The Company is engaged more often than usual in Data Processing to support the interests of the involved.

• Data Processing Required to Fulfil a Legal Obligation to Which the Data Controller is Subject (Legal Obligation)

The purpose of data processing based on legal obligation is to fulfil the obligations set forth in the relevant legal provisions and to enforce rights. The extent and duration of data processing based on legal obligations are determined by the applicable laws. Many legal provisions require the processing of personal data, which is inextricably linked to compliance. It is important to note that legal obligations are not optional, and they must be fulfilled in all cases.

• Data Processing Necessary to Protect the Vital Interests of the Data Subject or Another Natural Person

In special cases where the Data Subject is unable to protect their own interests or is otherwise incapacitated, data may be processed to the extent necessary and only for the duration of the impediment to protect vital interests.

• Data Processing Carried Out in the Public Interest or in the Exercise of Official Authority Vested in the Data Controller (Official Data Processing)

Since the Company is not an authority, it does not conduct data processing based on this legal basis.

• Data Processing Necessary for the Legitimate Interests Pursued by the Data Controller or a Third Party (Legitimate Interests)

The legal interest is typically based on a right stipulated in legislation or an agreement, and it is a justifiable interest from a business perspective. However, it is important to note that this is an option, not an obligation, unlike data processing based on legal obligations.

Data processing based on legitimate interests typically includes data processing related to promoting the Company's activities, optimizing services on the website/electronic interface, and collecting information related to the use of services (e.g., using cookies).

It is a requirement for data processing based on legitimate interests that the interests of the Company or a third party override the Data Subject's interests or fundamental rights and freedoms that require personal data protection (especially if the Data Subject is a child).

In all cases where data processing is based on the legitimate interests of the Company or a third party, the Company conducts a so-called balancing test to determine the permissibility of data processing. The essence of the balancing test is that the Company identifies the goal it wants to achieve, the possible means to achieve it, and then examines the rights and legitimate interests of the Data Subjects in opposition to the interests, and data can only be processed if the legitimate interest of the Company or the third party outweighs the legitimate interest of the Data Subject.

The Company documents the balancing test in writing, and information about it can be requested by the Data Subject.

The Company processes data directly provided by Data Subjects, data publicly available in databases (such as data in business partners' company extracts/individual entrepreneurs' records), and data lawfully made available by third parties.

1.4. GENERAL INFORMATION ABOUT THE COMPANY'S DATA PROCESSING

The Data Controller has an obligation to provide Data Subjects with concise, transparent, clear, and easily accessible information about the processing of their personal data in a manner that is clear and understandable.

The Company fulfils this information obligation by accepting and publishing this Regulation, as well as making a brief data processing information available at the time of data collection.

If you have any questions or wish to exercise your rights as described in this document or in the individual privacy notices, please contact us.

a) The official contact details of the Company are provided at the end of this Regulation and are also included in every individual data processing privacy notice.

b) The details of Data Processors used during data processing are provided at the end of this Regulation, and in the "Recipients" column of each data processing case, the category of the Data Processor related to that specific data processing (indicated by the services they provide) is briefly specified. Data Processors can only be individuals or businesses who commit to data processing tasks through written contracts, and they provide adequate guarantees for compliance with GDPR requirements and the protection of Data Subjects' rights through appropriate technical and organizational measures (the purpose, legal basis, tasks, and conditions of data processing, including necessary security measures, are determined by the Company). Data processors are not authorized to use the processed data for their own purposes. The Data Processor shall not engage any other data processor without the prior

written authorisation, on a case-by-case or general basis, of the Data Controller. In the case of a general written authorisation, the Data Processor shall inform the Data Controller of any planned changes affecting the use of additional data processors or their replacement, thereby giving the Controller the opportunity to object to those changes.

c) The Company is not obliged to appoint a data protection officer according to Article 37(1) of the GDPR. If such an appointment is made, the Data Controller will provide appropriate information about it.

d) The purpose and legal basis of data processing are specified in the Specific section for each individual data processing case. If data processing is based on the legitimate interest of the Company or a third party, this specific legitimate interest is defined in the Specific section.

e) The Specific section also specifies who can access and may have access to the processed personal data, to whom, and for what purposes (data recipients).

Regarding data transfer, the Company informs Data Subjects of the following:

• The Company may transfer the personal data it processes to courts and authorities for the purpose of fulfilling its contractual obligations and asserting its rights, depending on the nature of the data. In addition, compliance with certain legal obligations may involve data transfer (e.g., forwarding invoices, document content to the tax authority, reporting suspicions of money laundering, during authority inspections, if necessary).

• The Company is also entitled to transfer data to courts and authorities to assert its legitimate interests (e.g., claims for payment, data required for reporting suspected crimes, etc.).

• The Company is entitled to use Data Processors to fulfil its obligations and assert its rights (hosting service provider, accountant, administrative service provider). The list of these data processors is provided at the end of this Regulation.

• The Company only transfers personal data to areas outside the EEA (e.g., third-country hosting service provider, client) if the relevant country has a decision on adequacy issued by the European Commission or if data transfer is carried out with appropriate and adequate guarantees. Data Subjects can request information about the latter at any time from the Data Controller, including detailed information.

f) The duration of individual data processing and the retention period of data/documents are also specified in the Specific section for each data processing case. If the exact duration cannot be determined for a data/document, the criteria for determining the duration will be specified.

g) Data Subjects can request access to their personal data, correction, deletion, or restriction of processing from the Data Controller as detailed below, and they have the right to object to the processing of such personal data. In certain cases, they have the right to data portability. In the case of processing based on consent, consent can be withdrawn at any time, free of charge. Data Subjects have the right to lodge a complaint with the supervisory authority regarding

data processing. The rights of Data Subjects related to data processing are detailed in the following section.

h) When processing data of Data Subjects:

(i) When data processing is based on a legal obligation, the obligation to provide personal data is prescribed by law, and in such cases, Data Subjects are required to provide the data.

(ii) When data processing is carried out to fulfil a contractual obligation, the provision of data is based on a contractual obligation. If in such cases, providing data is a prerequisite for entering into a contract, this fact will be indicated separately in the Specific section.

(iii) In the case of data processing based on legitimate interests, Data Subjects may object to data processing at any time. In such cases, if the data cannot be processed on another legal basis and there are no compelling legitimate reasons that take precedence over the interests, rights, and freedoms of the data subject, the data will be deleted.

1.5 RIGHTS RELATED TO DATA PROCESSING FOR DATA SUBJECTS

Right of Access: The Data Subject has the right to request confirmation from the Data Controller as to whether their personal data is being processed and, if so, access to the following information:

- The purposes of the data processing.
- Categories of personal data concerned.
- Recipients or categories of recipients to whom the personal data has been or will be disclosed, including recipients in third countries or international organizations.
- If possible, the planned duration of the personal data storage, or if not possible, the criteria used to determine this period.
- The Data Subject's right to request the correction, deletion, or restriction of their personal data and to object to the processing of such data.
- The right to lodge a complaint with a supervisory authority.
- If the data was not collected from the Data Subject, all available information about its source.
- Whether automated decision-making or profiling is taking place.
- If personal data is transferred to a third country or an international organization, the right to be informed about the appropriate safeguards for such transfers.

If you want to know whether the Company is processing your personal data and under what circumstances, you can request this information.

The Company shall provide the data subject with a copy of the personal data processed upon request. It may charge an administrative fee for additional copies requested by the data subject. If the data subject has made the request by electronic means, the information shall be provided in a commonly used electronic format, unless the data subject requests otherwise.

Right to Rectification: The Data Subject has the right to request the Data Controller to promptly correct any inaccurate personal data concerning them. Taking into account the

purpose of data processing, the Data Subject is entitled to request the completion of incomplete personal data, including through the provision of a supplementary statement.

Please inform us if any of your personal data changes so that we can update it in our records.

The Data Controller shall inform all recipients to whom or with whom the personal data have been disclosed of the rectification, unless this proves impossible or involves a disproportionate effort. At the request of the data subject, the Dara Controller shall provide information on those recipients.

Right to Erasure ("Right to be Forgotten"): The Data Subject has the right to request the Data Controller to erase their personal data without undue delay if one of the following reasons applies:

- The personal data is no longer necessary for the purposes for which it was collected or otherwise processed (the purpose of data processing has been fulfilled).
- The Data Subject withdraws their consent, and there is no other legal basis for the data processing.
- The Data Subject objects to the data processing based on the legitimate interests of the Data Controller, and there are no overriding legitimate grounds for the processing, or the Data Subject objects to direct marketing.
- The personal data has been unlawfully processed.
- The erasure of personal data is required to comply with a legal obligation under EU or Member State law.
- The personal data has been collected in relation to the offer of information society services to a child.

If the Data Controller has made the personal data public, it will take reasonable steps, including technical measures, to inform data processors processing the personal data that the Data Subject has requested the erasure of any links to, or copies or replication of, the personal data.

The right to erasure does not apply when the data processing is necessary:

- For exercising the right to freedom of expression and information.
- For compliance with a legal obligation.
- For the performance of a task carried out in the public interest or in the exercise of official authority.
- For reasons of public interest in the area of public health.
- For archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes.
- For the establishment, exercise, or defence of legal claims.

If you believe that the conditions for erasure are met, you can request the deletion of your data at any time.

Right to Restriction of Processing: The Data Subject has the right to request the Data Controller to restrict the processing of their personal data if one of the following applies:

- The accuracy of the personal data is contested by the Data Subject, for a period enabling the Data Controller to verify the accuracy of the personal data (i.e., while its accuracy is being verified).
- The processing is unlawful, and the Data Subject opposes the erasure of the personal data and requests the restriction of its use instead.
- The Data Controller no longer needs the personal data for the purposes of processing, but it is required by the Data Subject for the establishment, exercise, or defense of legal claims.
- The Data Subject has objected to processing pending the verification of whether the legitimate grounds of the Data Controller override those of the Data Subject.

During a restriction period, personal data may only be processed with the Data Subject's consent or for the establishment, exercise, or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest. The Data Controller will inform the Data Subject before lifting a processing restriction.

If you request the restriction of data processing, the processing of your data will be limited to storage, and it will only be processed further with your consent or for specific legal purposes.

Right to Data Portability: The Data Subject has the right to receive their personal data provided to the Data Controller in a structured, commonly used, and machine-readable format, and to have it transmitted to another Data Controller, provided that the processing is based on the Data Subject's consent or is necessary for the performance of a contract, and the processing is carried out by automated means.

When exercising the right to data portability, the Data Subject has the right to request the direct transmission of their personal data between Data Controllers, if technically feasible.

Right to Object: The Data Subject has the right to object, on grounds relating to their particular situation, at any time to processing of personal data concerning them, including profiling based on those provisions. The Data Controller shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights, and freedoms of the Data Subject or for the establishment, exercise, or defence of legal claims.

If personal data is processed for direct marketing purposes, the Data Subject has the right to object at any time to the processing of their personal data for such marketing, including profiling related to such direct marketing.

If you object to the processing of your personal data, the data will no longer be processed for such purposes.

Automated Individual Decision-Making, Including Profiling: The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

The above does not apply if the decision:

- Is necessary for entering into or performing a contract between the Data Subject and the Data Controller.
- Is authorized by EU or Member State law to which the Data Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights, freedoms, and legitimate interests.
- Is based on the Data Subject's explicit consent.

Filing a complaint with the supervisory authority, legal proceedings: Without prejudice to any other administrative or judicial remedies, every Data Subject shall have the right to lodge a complaint with a supervisory authority, in particular in the Member State of their habitual residence, place of work, or place of the alleged infringement, if the Data Subject considers that the processing of personal data relating to them infringes the provisions of the GDPR.

The subject matter of the complaint shall be investigated by the supervisory authority, and the complainant shall be informed of the progress and outcome of the investigation within a reasonable period, in particular if further investigation or cooperation with another supervisory authority is necessary.

As a result of the complaint, the supervisory authority is entitled to initiate proceedings against the Data Controller. If the Data Controller does not take measures in response to the Data Subject's request, the Data Subject shall be informed without undue delay, but no later than one month after the request is received, of the reasons for the absence of action and of the possibility of lodging a complaint with a supervisory authority and seeking judicial remedy.

The precise contact information for the Hungarian supervisory authority is provided at the end of this Regulation.

Limitations: Union or Member State law may restrict the rights of Data Subjects as set out above when legislative measures are necessary for the protection of the Data Controller or processor.

Record keeping: The Data Controller maintains a record of communications from Data Subjects and the responses thereto.

Judicial enforcement, compensation, and damages: The Data Subject may bring an action against the Data Controller or, as the case may be, against the data processor in a court if the Data Subject considers that the processing of personal data relating to them infringes the provisions of the GDPR or other data protection laws. It is the responsibility of the Data Controller (or data processor) to demonstrate compliance with the provisions. The Data Subject may bring the action before the courts of the Member State where they have their habitual residence or where they work. A Data Subject may be a party to the proceedings even if they do not have a place of domicile or habitual residence in the Member State in question. The Data Protection Authority may intervene in proceedings to support the Data Subject in obtaining a judgment in their favour.

If the Data Controller, by processing the Data Subject's data unlawfully or by breaching data security requirements, causes damage to another party, they shall be obliged to make reparation. If the Data Controller, by processing the Data Subject's data unlawfully or by breaching data security requirements, infringes the Data Subject's right to personality, the Data Subject may claim compensation from the Data Controller.

The Data Controller is liable to the Data Subject for damage caused by the data processor's actions, and the Data Controller shall also pay the Data Subject damages if the data processor infringes the Data Subject's right to personality by processing their data. The Data Controller is exempt from liability for the damage caused and from the obligation to pay damages if they prove that the damage or infringement of the Data Subject's right to personality resulted from an unavoidable cause outside the scope of data processing. No compensation shall be paid for damage, and no damages may be claimed insofar as the damage or infringement of the right to personality of the Data Subject resulted from the intentional or grossly negligent conduct of the Data Subject.

1.6. REQUIREMENTS FOR DATA SECURITY

The Company stores personal data electronically and/or on paper, with specific information provided in the Specific Section.

To ensure the security of data, the Company employs appropriate organizational and technical measures. When determining the appropriate level of security, particular attention is paid to the risks arising from data processing, in particular those resulting from the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data.

Data stored electronically is stored on servers owned by the server service provider Websupport Magyarország Kft. These servers are located within the European Union. Archived documents are archived by the external service provider Websupport Magyarország Kft. The email system is provided by [Google Workspace and Websupport Magyarország Kft.

The computers and workstations used by the Company are password protected, with access to documents restricted based on access rights management rules. All computer systems of the Company are protected against malicious software.

Data is regularly backed up with continuous overwriting. The physical document storage room is protected against water, fire, and unauthorized access.

To ensure compliance with data security requirements, the Data Controller provides instructions and regulations in addition to this Regulation. The Data Controller ensures that the current content of this Regulation, as well as any additional instructions and regulations, is made known to its members and third parties acting within its sphere of interest (especially data processors), and that they act accordingly.

1.7. DATA TRANSFER

Personal data processed by the Company may only be transferred to the following recipients and only in the following cases:

a) to a data processor or another Data Controller for the purpose of achieving the data processing objectives;
b) to any recipient with the consent of the Data Subject;
c) pursuant to a legal obligation or an official order, to the recipients specified by law;
d) in the event of suspicion of a criminal offense or upon request, to the investigating authority, as well as to the authority conducting the proceedings for the offense and the authority conducting the preparatory proceedings for the offense;
e) in case of facilitating the business interest of the involved.

1.8. DATA PROCESSING

In order to ensure its operations, the Company may engage various services (e.g., administrative service providers, postal services, accountants, couriers, business partners of the ecosystem etc.). Such services often involve the processing of personal data.

When availing of such services, the Company acts as the Data Controller, while the service provider acts as the data processor.

The Company will only engage data processors who provide adequate guarantees for compliance with GDPR requirements and the implementation of appropriate technical and organizational measures to protect the rights of Data Subjects.

The rights and obligations of the data processor regarding the processing of personal data, under the framework of GDPR and relevant data processing laws, are determined by the Data Controller, which means the Company specifies to the data processor(s) what operations they should perform with what data. The lawfulness of these instructions is the responsibility of the Data Controller. The data processor may engage additional data processors in accordance with the instructions of the Data Controller.

The data processor cannot make substantive decisions regarding data processing, can only process personal data in accordance with the instructions of the Data Controller, cannot engage in data processing for its own purposes, and must store, retain, or delete personal data as required by the Data Controller.

The agreement related to data processing must be in writing and specify at least the subject matter, duration, nature, and purpose of the processing, the types of personal data, categories of Data Subjects, and the Data Controller's GDPR obligations and rights, as well as its responsibilities. According to applicable legal provisions, an organization engaged in a business activity related to the processed personal data cannot be entrusted with data processing.

Detailed information about the data processors contracted by the Company is provided in Appendix 1 at the end of this Regulation.

2. SPECIAL SECTION

1. Supplier and Service Partner Data

Like any economic entity, the Company processes the data of individuals (including legal representatives in the case of legal entities) who have or intend to establish a supplier or service partner relationship with it, for the purpose of conducting contracts and fulfilling related obligations (organizing procurement, invoicing/payment, etc.) in connection with its activities.

The processing of data related to contracts with suppliers and service partners involves, on one hand, the physical archiving of contract copies, documents/invoices (at the Company's headquarters), and on the other hand, electronic backup of the data.

In business partner relationships, the Data Controller does not accept cash payments exceeding 3 million HUF (only bank transfers). Therefore, for this reason, the Data Controller is not required to perform customer identification under the Anti-Money Laundering Act (Pmt.). If such a requirement arises, the Data Controller will provide separate information to the Data Subject regarding the details of the identification under the Pmt.

The summary description of the data processing for individual suppliers and service partners is presented in Table 1.

2. Data Processing Related to Main Activities (Asset Management / Holding / Venture Capital) (Portfolio, Investors)

Most data processing related to the Data Controller's main activities takes place within the Company's IT System (hereafter: "System"), which is an internet-accessible platform developed and operated by Growth Masters Kft..

2.1. Startups

2.1.1. Registration in the System, Filling out Investment Application Form

Innovators with technological innovations (hereafter: "Founders") who wish to present their projects have the opportunity to register, apply for programs and apply to be involved in the cooperation with the Company’s business partners by filling out an application form available on the https://obudaunivc.com/jelentkezz website.

As part of the registration as a founder, founders can apply for investment by filling out a form in the System, providing the following data: (i) project/startup name; (ii) founder's name, email address, phone number; (iii) LinkedIn profile link; (iv) OnePager; (v) Pitch Deck (optional); (vi) Pitch video (optional).

Among the information listed above, the data of the founder and team members can be considered personal data.

If any other documents are uploaded, which are not necessarily required but the founders wish to share, the Data Controller requests careful consideration in terms of data protection awareness and asks that they only share such documents if they have the

authorization to do so, considering that the founder is responsible for the legality of sharing the data.

2.1.2. Rejection Letter

After the application, the Data Controller verifies the submitted documents and responds to the request within a reasonable time, which may be up to 30 days depending on the Company's internal processes. If the Data Controller does not find the project suitable for investment, a rejection letter is sent to the email address provided during the application.

2.1.3. Signed Term Sheet

After approving the application, the Company initiates negotiations regarding collaboration, for which a Term Sheet is prepared. In case of agreement, a written term sheet is signed, which is a preliminary contractual condition draft containing essential legal provisions, but does not have mandatory legal force regarding the merits of the investment. However, it is necessary for the signing of the final investment agreement.

2.1.4. Due Diligence, Due Diligence Report

Following the signing of the term sheet, a due diligence process begins, during which the Company thoroughly reviews/has reviewed the company/project in detail for its final investment decision. The due diligence process generally includes legal, financial, and professional review. As a result of the due diligence process, a due diligence report (DD Report) is prepared.

2.1.5. Investment Phase: Syndicate Agreement and Corporate Amendment Documents

After a successful due diligence process, the availability of the investment is made through the Data Controller's equity investment in the invested company. Accordingly, syndicate agreements and corporate amendment documents are prepared and signed by the parties with the content required by the Commercial Court.

2.1.6. Implementation, Reporting Phase, Financial Settlement

After a successful investment, reports on the progress and developments of the project are prepared based on the data provided by the Data Subject. This includes documentation of financial settlements between the Data Controller and the Data Subject, as well as the invested company.

2.2. Handling of Investor Data

In the course of its business activities, the Data Controller is in contact with potential investors (hereafter: "Investors") who wish to participate as investors in the Data Controller's venture capital investments.

Individuals applying as investors can contact the Data Controller through the Company's employees or direct email inquiries.

Providing personal data is entirely voluntary, but without it, the application of a person applying as an investor cannot be evaluated. Therefore, it is recommended to signal data protection and data processing concerns in this case.

2.2.1. Investment Agreement

In the case of successful negotiations, an investment agreement is concluded between the Investor and the Data Controller.

2.2.2. Presentation of Investors on the Website

After signing the investment agreement, investors have the opportunity to be featured on the https://obudaunivc.com/ website.

2.2.3. Financial Settlements

Based on the investment agreement, a financial settlement obligation may arise between the Data Controller and the Investor.

The summary description of data processing related to the main activities (portfolio companies, investor partners) is presented in Table 2.

3. Other Data Processing

3.1. Handling of Incoming Written Inquiries and Electronic Inquiries, Outgoing Mail Handling

Incoming inquiries to the central mailing address and contact@obudaunivc.com email address are received and processed by authorized Company employees within the Data Controller's organization, including the handling of any personal data mentioned in the inquiries. Incoming written inquiries are electronically archived according to separate document management rules and forwarded to the relevant officer, and are also archived in paper format. Email messages containing inquiries are manually sorted and forwarded to authorized officers, and after that, the inquiries are manually deleted from the inbox.

For outgoing mail (both local and central mailings), postal receipts and return receipts are created and, upon their return, are archived along with the respective letters as proof of dispatch.

The retention period for incoming inquiries depends on the type of case specified in this Data Processing Notice.

3.2. Handling of Website Visitors' Data - Cookies

The use of cookies allows for the retrieval of certain visitor data and the recording of internet usage habits. In general, cookies can facilitate the use of a website, help provide relevant

information to the visitor, and ensure proper supervision of the site's operation by the site operators (e.g., preventing misuse and ensuring the proper provision of services on the site).

Upon entering the https://obudaunivc.com/ website, if the visitor's web browser settings allow it or if the visitor explicitly approves it during the first visit to the website, the website will automatically save information using these cookies.

Consent to the use of cookies is voluntary. Generally, you can disable cookies through the Tools/Settings menu of your browser, under data protection and/or cookies, and a window will automatically pop up during the website's first visit, drawing attention to cookies.

The detailed description of cookies used by the Data Controller can be found directly on the respective pages.

Please note that cookies themselves cannot identify the visitor to the website, and the Data Controller does not take steps to identify individuals.

3.3. Other Data Processing Not Specified in this Regulation

The Data Controller may conduct data processing not detailed in this Data Processing Notice. In each case, before such data processing, the Data Controller provides information to the Data Subjects, and these data processing activities are also covered by this Regulation.

Disclaimer: This Privacy Policy is a true and accurate translation of the Company's privacy policy (in Hungarian: Adatkezelési Szabályzat és Tájékoztató) in case of any discrepancy between the original and the translation, the Hungarian version shall prevail.

***

Authority details and contact information:

Name: Hungarian National Authority for Data Protection and Freedom of Information (Nemzeti Adatvédelmi és Információszabadság Hatóság)

Abbreviated name: NAIH

Address: 9-11 Falk Miksa Street, 1055 Budapest, Hungary

Mailing address: Pf. 9, 1363 Budapest, Hungary

Phone: +36-1-391-1400 Fax: +36-1-391-1410

Email:ugyfelszolgalat@naih.hu

This Regulation is effective from September 1, 2023, until revoked or modified. The Company reserves the right to change this Regulation. The Company provides information on this Regulation and its interpretation in electronic form. Questions related to this can be sent to the contact address below:

Data Controller's Contact Information: Registered and mailing address:

1034 Budapest, Bécsi út 96/B.

Email: contact@obudaunivc.com

1. Suppliers, service providers

Description of the data processing	Processed Data	Purpose of the processing	Legal basis	Source	Recipient	Timing
Processing natural person contractual partner's data (IDENTIFICATION)	Name Address Mother's name Sole proprietor registry number, tax number Name card details Bank account number	Identification of the contractual party	Performance of a contractual obligation Article 6 GDPR (1)(b)	Data Subject	Portfolio management service provider Server provider IT system provider	In the case of personal data contained in the documents necessary to establish the content of the contract or to prove performance, 5 years after the termination of the contract (general limitation period). In other cases, personal data will be deleted immediately after the termination of the contract or of the representative's capacity.
Processing natural person contractual partner's data (CONTACT)	E-mail Phone number In case of Contact Person: Name E-mail Telephone Position Name card details	Maintaining contact with the contractual party	Performance of a contractual obligation Article 6 GDPR (1)(b) legitimate interest in ensuring the contractual relationship	Data Subject If a contact is indicated, the data source is the contractual partner GDPR Art 6 (1) f)	Portfolio management service provider Server provider IT system provider	In the case of personal data contained in the documents necessary to establish the content of the contract or to certify performance, 5 years after the termination of the contract (general limitation period). In other cases, personal data will be deleted immediately after the termination of the contract or the termination of the capacity of representative.
Processing natural person contractual partner's data (BILLING)	Billing information	Invoicing	Accountancy Act, Art. 165-169. – GDPR Art 6 (1) c) pont	Data Subject	Portfolio management service provider Server provider IT system provider	8 years from the last day of the year in which the certificate was issued.

Processing legal person contractual partner's data (IDENTIFICATION)	Name of the Representative Address Mother's name Sole proprietor registry number, tax number Name card details Bank account number	Identification of the contractual party	Performance of a contractual obligation Article 6 GDPR (1)(b)	Data Subject	Portfolio management service provider Server provider IT system provider	In the case of personal data contained in the documents necessary to establish the content of the contract or to prove performance, 5 years after the termination of the contract (general limitation period). In other cases, personal data will be deleted immediately after the termination of the contract or of the representative's capacity.
Processing legal person contractual partner's data (CONTACT)	E-mail Phone number In case of Contact Person: Name E-mail Telephone Position Name card details	Maintaining contact with the contractual party	Legitimate interest in ensuring the contractual relationship - GDPR Art 6 (1) f)	Data Subject or if different from the representative, the source of the data is the legal person representative of the legal entity	Portfolio management service provider Server provider IT system provider	In the case of personal data contained in the documents necessary to establish the content of the contract or to certify performance, 5 years after the termination of the contract (general limitation period). In other cases, personal data will be deleted immediately after the termination of the contract or the termination of the capacity of representative.
Processing legal person contractual partner's data (BILLING)	Billing information	Invoicing	Accountancy Act, Art. 165-169. – GDPR Art 6 (1) c) pont	Data Subject	Portfolio management service provider Server provider IT system provider	8 years from the last day of the year in which the certificate was issued.

2. Data processing relating to main activities

Description of the data processing	Processed Data	Purpose of the processing	Legal basis	Source	Recipient	Timing
Registration / Application	Founder's data (name, contact details, email, telephon) Project name Project description Marketing materials (OnePager, Pitch Deck)	Search and selection for investment	Data Subject consent (GDPR Art 6. (1) a))	Data Subject	Website service provider IT system provider	Registration data will be kept until consent is withdrawn. In case of refusal, in the absence of withdrawal, the Founder's profile and the documents submitted will be deleted after 5 years. In case of acceptance, the provisions applicable to the data accepted will apply..
Rejection letter	Founder's name Founder's e- mail	Notice to the applicant	Legitimate interest: providing notice to Applicants (GDPR Art 6 (1) f))	Data Subject	Portfolio management service provider Server provider Website service provider IT system provider Email service provider	Rejection letters are stored together with the Application data (5 years)

Video	Video recording (audio and video) with the Founder and team members	Search and selection for investment	Legitimate interest: search and selection of applicants (main activity of the Company) to Applicants (GDPR Art 6 (1) f))	Data Subject, the persons present in the video	Portfolio management service provider Server provider Website service provider IT system provider	Videos are stored together with the Application data (5 years)
Term sheet	Term sheet content: including details of parties' representatives (name, position, title, business contact details, signature); details of members and key persons: (name, position).	Search and selection for investment Taking the necessary steps to conclude a contract, identifying the possible contractual terms	In case of data of representatives of the contracting parties: contractual obligation, taking the necessary steps to conclude the contract at the request of the Data Subject (GDPR Art 6 (1) b)) Members and key persons who do not sign the document: Legitimate interest: clarification of contractual terms (GDPR Art 6 (1) f))	Data Subject, or, for members/key persons other than the Applicant/Founder, the source of the data Applicant/ Founder	Portfolio management service provider Server provider Website service provider IT system provider	In the case of a final investment agreement, the term sheet is kept with the final agreement In the absence of a final investment agreement, the term sheet is kept for 5 years

Due Diligence (DD Report)	Details of founders/members: (name, address, date and place of birth, mother's name, tax identification number, date of membership, position held in the company) Employees' details: content of employment contracts (name, date and place of birth, address, mother's name, social security number, tax identification number, date of employment, any other details recorded in the employment contract) details of contractual partners: content of partner contracts: (Representative: name, position, signature, Contact: name, business telephone number, e-mail address) Content of DD report	Conducting due diligence	Legitimate interest: conducting due diligence (GDPR Art 6 (1) f))	Data Subject, or in the case of members/employers, contractors who are not the Applicant/Founder, the source of the data is the Applicant/Founder	Portfolio management service provider Server provider Website service provider IT system provider Financial expert involved in the due diligence process The legal expert involved in the due diligence as a separate data controller	In case of a final investment agreement, the due diligence data will be kept with the final agreement In the absence of a Final Investment Agreement, the Due Diligence Data will be retained for 5 years.

Final investment documents - syndicate contract, company modification documents	Members of the Invested Company: name, address, date of birth, mother's name, tax identification number, date of membership For the representatives of the Invested Company: name, address, date of birth, mother's name, tax identification number, date of beginning of representation	Documentation of the investment, preparation of the documents required for the change of company name	Performance of a contractual obligation Article 6 GDPR (1)(b)	Data Subject, or, for any member or representative who is not the Applicant/Founder, the source of the data is the Applicant/Founder	Portfolio management service provider Server provider Website service provider IT system provider The legal expert involved in the drafting of the document and in the company law procedure, as an independent data controller Company Court as an independent data controller The data will be published publicly in the Companies Register, so that they cannot be be made available to predeterminable third parties	Duration of the Data Controller's operation

Reports	Name of the representative of the invested company Shareholders of the invested company /members of the company	Follow up of the contract	Performance of a contractual obligation Article 6 GDPR (1)(b)	Investee company	E-mail provider Portfolio management service provider Server provider Website service provider IT system provider Investors as Joint data controllers	5 years after exit from the investee company
First e-mail contact	Name E-mail Other voluntarily shared data	Maintaining connection with the data subject	Data Subject consent (GDPR 6. (1) a)) given by sending the first contact e-mail to the Data Controller, as an active behaviour, to the Data Controller.	Data Subject	Portfolio management service provider Server provider E-mail provider	If the Data Subject who has applied to become an Investor does not register in the System and no further cooperation and investment agreement is established, the first contact e-mail will be deleted after 30 days.
Investment documentation	Investor details: In case of a natural person investor: Name, Address, Mother's name, Place and date of birth, Tax identification number	A create the contractual documentation required for the investment	Contractual obligation (GDPR 6. (1) b)	Data Subject	Portfolio management service provider Server provider Website service provider IT system provider Legal	Duration of the Data Controller's operation

Introduction of the Investor	In the case of a company: Name, position and signature of company representative Investor's name Photo CV or LinkedIn profile, website	Introduction of the Investor	Data Subject consent (GDPR 6. (1) a))	Data Subject	Portfolio management service provider Server provider Website service provider IT system provider	Until revoked Until the cooperation with the Investors
Handling incoming requests	Any personal data recorded by the sender in the request	Handling incoming requests	Legitimate interest in the lawful operation of the Company to deal with enquiries (GDPR Art 6 (1) f)) In case of a contractual relationship, incoming requests will be treated on the legal basis of the performance of a contractual obligation (GDPR Art 6 (1) b))	Data Subject	Portfolio management service provider Server provider IT system provider	Handling incoming requests

Outgoing mail items and return items	Addressing data	Recording outgoing mail items and return items	Legitimate interest in proving that correspondence has taken place (GDPR Art 6 (1) f))	Company records	Portfolio management service provider	Outgoing mail items and return items

1. **Appendix – List of Data Processors**

Activity	Name	Seat	Registration no.	Telephone	E-mail
Portfolio management	Óbuda Uni Venture Capital Zrt.	1034 Budapest, Bécsi út 96/B	01-10-142341	-	contact@obudaunivc.com
Portfolio management, supervision	Óbudai Egyetem	1034 Budapest, Bécsi út 96/B	FI 12904	36 (1) 666-560	i
Server service provider, archives	Websupport Magyarország Kft.	1132 Budapest, Victor Hugo utca 18-22.	01-09-381419	06 1 700 2323	info@mhosting.hu
Website operator	Websupport Magyarország Kft.	1132 Budapest, Victor Hugo utca 18-22.	01-09-381419	06 1 700 2323	info@mhosting.hu
IT system operator	Growth Masters Kft.	7632 Pécs, Maléter Pál u. 44. 2. ajtó	02-09-085656	70/510-2272	andras@growthhackers.hu
Legal	dr. Bence Spiczmüller, attorney at law	1088 Budapest, Bródy Sándor utca 32. fszt. 5.	KASZ: 36068616	70/243-4119	bence.spiczmuller@avocat.hu
Marketing és PR counsel	Growth Masters Kft.	7632 Pécs, Maléter Pál u. 44. 2. ajtó	02-09-085656		andras@growthhackers.hu
Auditor	UNIKONTO Számvitelkutatási Kft.	1093 Budapest, Fővám tér 8. III/317.3	01-09-073167	70/510-2272	*lakatos@uni-corvinus.hu*