Privacy Policy and Notice

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 our partners regarding V4-Ukraine Talent Fusion Igniting Innovation Amidst Adversity Project "Project" in contact with them (hereinafter referred to as "Users"). Respecting their right to self-determination in connection with data handling is of paramount importance.

The web address of the Project is https://www.talentfusion.eu/ ("Website") and the Company's web address is: https://obudaunivc.com/.

This privacy policy will explain how our organisation uses the personal data the Company collects from the User.

I. General Notice

A. Types of Data collected

Among the types of personal data that talentfusion.eu website collects, by itself or through third parties, there are: basic details of the User, including, but not limited to first name, surname, e-mail, telephone number, and address; as well as other details necessary for the Project, allowing for the determination of identity either directly or indirectly "Personal Data".

Personal Data may be freely provided by the User, or, in case of Usage Data, collected automatically when using the Website.

Users who are uncertain about which Personal Data is mandatory are welcome to contact the Company.

Users are responsible for any third-party Personal Data obtained, published or shared through the Website and confirm that they have the third party's consent to provide the Data.

B. Who we share your data with

We are sharing your personal data actively with Project partners:

Accelpoint Sp. z o.o.

Street, house no.: ul. Mokotowska 1

Town: Warsaw

Postal code: 00-640

Country: Poland

Громадська спілка "рівне іт кластер" (RIVNE IT CLUSTER)

Street, house no.: 25 Zakhysnykiv Mariupola street

Town: Rivne

Postal code: 33022

Country: Ukraine

Insane Business Ideas s.r.o.

Street, house no.: Všehrdova 437/15

Town: Praha

Postal code: 118 00

Country: Czechia

C. Legal basis of processing

The Company may process Personal Data relating to Users if one of the following applies:

- Users have given their consent for one or more specific purposes. Note: Under some legislations the Company may be allowed to process Personal Data until the User objects to such processing (“opt-out”), without having to rely on consent or any other of the following legal bases. This, however, does not apply, whenever the processing of Personal Data is subject to European data protection law;
- provision of Data is necessary for the performance of an agreement with the User and/or for any pre-contractual obligations thereof;
- processing is necessary for compliance with a legal obligation to which the Company is subject;
- processing is related to a task that is carried out in the public interest or in the exercise of official authority vested in the Company;
- processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party.

In any case, the Company will gladly help to clarify the specific legal basis that applies to the processing, and in particular whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract.

D. Place of processing

The Data is processed at the Company's operating offices and in any other places where the parties involved in the processing are located.

Depending on the User's location, data transfers may involve transferring the User's Data to a country other than their own. To find out more about the place of processing of such transferred Data, Users can check the section containing details about the processing of Personal Data.

Users are also entitled to learn about the legal basis of Data transfers to a country outside the European Union or to any international organisation governed by public international law or set up by two or more countries, such as the UN, and about the security measures taken by the Company to safeguard their Data.

If any such transfer takes place, Users can find out more by checking the relevant sections of this document or inquire with the Company using the information provided in the contact section.

E. Retention time

Personal Data shall be processed and stored for as long as required by the purpose they have been collected for.

Therefore:

- Personal Data collected for purposes related to the performance of a contract between the Company and the User shall be retained until such contract has been fully performed.
- Personal Data collected for the purposes of the Company’s legitimate interests shall be retained as long as needed to fulfill such purposes. Users may find specific information regarding the legitimate interests pursued by the Company within the relevant sections of this document or by contacting the Company.

The Company may be allowed to retain Personal Data for a longer period whenever the User has given consent to such processing, as long as such consent is not withdrawn. Furthermore, the Company may be obliged to retain Personal Data for a longer period whenever required to do so for the performance of a legal obligation or upon order of an authority.

Once the retention period expires, Personal Data shall be deleted. Therefore, the right to access, the right to erasure, the right to rectification and the right to data portability cannot be enforced after expiration of the retention period.

F. The purposes of processing

The Data concerning the User is collected to allow the Company to provide its Service, comply with its legal obligations, respond to enforcement requests, protect its rights and interests (or those of its Users or third parties), detect any malicious or fraudulent activity, as well as the following: Displaying content from external platforms, Contacting the User, Analytics and Platform services and hosting.

For specific information about the Personal Data used for each purpose, the User may refer to the section “Detailed information on the processing of Personal Data”.

G. What personal data we collect and why we collect it - Detailed information on the processing of Personal Data

The Personal Data is collected for the following purposes:

H. Contacting the User - Contact and feedback forms

We collect the data you enter and keep it stored in our email or CRM application, hosted by third parties. This data is used to collaborate with the User or provide the services the User is requesting.

Personal Data processed: email address; first name; last name; various types of Data.

I. Analytics

The services contained in this section enable the Company to monitor and analyse web traffic and can be used to keep track of User behaviour.

Personal Data processed: Cookies; Usage Data.

Place of processing: Ireland – **Privacy Policy** – **Opt Out**. Privacy Shield participant.

- Displaying content from external platforms

This type of service allows you to view content hosted on external platforms directly from the pages of the Website and interact with them.

This type of service might still collect web traffic data for the pages where the service is installed, even when Users do not use it.

Google Fonts (Google Ireland Limited)

Google Fonts is a typeface visualisation service provided by Google Ireland Limited that allows the Website to incorporate content of this kind on its pages.

Personal Data processed: Usage Data; various types of Data as specified in the privacy policy of the service.

Place of processing: Ireland – **Privacy Policy**. Privacy Shield participant.

Category of personal data collected according to CCPA: internet information.

This processing constitutes a sale based on the definition under the CCPA. In addition to the information in this clause, the User can find information regarding how to opt out of the sale at **https://ccpa-info.com**.

- Platform services and hosting

These services have the purpose of hosting and running key components of the Website, therefore allowing the provision of the Website from within a unified platform. Such platforms provide a wide range of tools to the Company – e.g. analytics, user registration, commenting, database management, e-commerce, payment processing – that imply the collection and handling of Personal Data.

Some of these services work through geographically distributed servers, making it difficult to determine the actual location where the Personal Data are stored.

J. What rights you have over your data

If you have an account on this site, have left comments, or submitted personal information via contact form / chat, you can request to receive an exported file of the personal data we hold about you, including any data you have provided to us. You can also request that we erase any personal data we hold about you. This does not include any data we are obliged to keep for administrative, legal, or security purposes.

- Additional rights of EEA residents

If you are a resident of a country in the EEA (European Economic Area), you have the right, among others, to:

(1) Access your personal data

(2) Ensure the accuracy of your personal data

(3) Ask us to delete your personal data

(4) Restrict further processing of your personal data

(5) Complain to a supervisory authority in your country of residence in the event that your data is misused

If you believe that our processing of your personal data has infringed data protection laws, you have a legal right to lodge a complaint with a supervisory authority responsible for data protection.

- How to exercise these rights

Any requests to exercise User rights can be directed to the Company through the contact details provided in this document. These requests can be exercised free of charge and will be addressed by the Company as early as possible and always within one month.

K. Changes to this Privacy Policy

Occasionally, it may be necessary for us to change the terms of this Privacy Policy. We will do so by posting updated text on the website, and your continued use constitutes the acceptance of any changes. To ensure you are aware of our current privacy practices, we recommend that you check this page periodically. We will not change how we handle previously collected

information without providing notice and an opportunity to choose how we use that information.

L. Information not contained in this policy

More details concerning the collection or processing of Personal Data may be requested from the Company at any time. Please see the contact information below.

Óbuda Uni Venture Capital Zrt.
Registered office address: 1034 Budapest, Bécsi út 96/B
CRN: 01-10-142341
TAX number: 32271557-2-41
e-mail: contact@obudaunivc.com

II. Privacy Policy

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR);

1. Definitions

The conceptual system of this Notice corresponds to the interpretative definitions set out in Article 4 GDPR, in particular:

- ***'data processing'*** means the performance of technical tasks associated with the processing operations of personal data, whether or not by automated means, irrespective of the means and method used for carrying out the operations and the location of such use, provided that the technical task is performed on the data;
- ***'data processor'*** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the data controller;
- ***'data processing'*** means 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- ***'data controller'*** means 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 controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- ***'data transmission'*** means the transmission of processed personal data to other Data Controllers for purposes other than data processing;
- ***'personal data breach'*** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
- ***'pseudonymisation'*** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific natural person without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to identified or identifiable natural persons;
- ***'consent of the data subject'*** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- ***'recipient'*** means 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 who may receive personal data in the framework of a particular inquiry by Union or Member State law should not be regarded as recipients; the processing of those

data by those public authorities should comply with the applicable data protection rules according to the purposes of the processing;

- ***'third party'*** means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;
- ***'special data'*** means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, as well as genetic and biometric data for the unique identification of natural persons, health data and personal data concerning the sexual life or sexual orientation of natural persons;
- ***'profiling'*** means 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;
- ***'personal data'*** means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person can be identified, directly or indirectly, in particular, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Any references in the Privacy Policy to:

1) **Controller** - shall mean the Company. The controller shall also mean the Controller of Personal Data in the meaning of the General Data Protection Regulation.

2) **Personal Data** - shall mean basic details of the User, including, but not limited to first name, surname, e-mail, telephone number, and address; as well as other details necessary to participate in the Project, allowing for the determination of identity either directly or indirectly;

3) **Project** – shall mean V4-Ukraine Talent Fusion Igniting Innovation Amidst Adversity Project;

4) **Controllers' Services** - shall mean additional services offered by the Controllers to the Users.

5) **Software** – shall mean computer programs that may be used by the User to browse the Website;

6) **Cookie files (the so-called cookies)** – shall mean IT data, in particular, text files, stored on the User's Device to browse websites on the Website;

7) **Personal Data Processing** – shall mean an operation or set of operations executed on personal data or sets of personal data in either automated or non-automated manner, such as gathering, recording, organising, ordering, storing, adapting or modifying, downloading, browsing, using, disclosing by transmission, disseminating or other sharing, matching or combining, deleting or destroying;

8) **Regulations** - shall mean the document specifying the types, scope and conditions for the organisation of the Project, as well as the rights and obligations of both Controller and Users;

9) **Registration** - shall mean the process of registration carried out by the Regulations by the User through the Website;

10) **Device** – shall mean the electronic device, through which the User gains access to the Website, in particular: PCs, laptops, tablets, smartphones;

11) **User** - shall mean the person, to whom electronic services are provided by the Regulations and the provisions of the law and who participates in the Project or uses one of the Controller's Services.

If the definitions of the GDPR in force at any given time differ from the definitions in this Notice, the definitions given in the Regulation prevail.

2. Principles of data processing

2.1 Principles of legality, due process and transparency

Personal data must be processed lawfully and fairly and transparently in relation to the Data Subject. In the interest of lawful data processing, it must be based on the consent of the Data Subject or must have another basis established by law.

Personal data may be processed only if the purpose of data processing cannot reasonably be fulfilled by other means.

Any information and communication relating to the processing of personal data must be easily accessible and easy to understand, and clear and plain language must be used.

To achieve fair, transparent data processing, it is necessary that the Data Subject is informed about the fact and purposes of data processing.

If the Company collects personal data directly from the Data Subject, it is necessary to inform the Data Subject whether they are obliged to disclose the personal data and what consequences non-disclosure may have on them. The information must be provided to the Data Subject at the time of data collection.

If the data were collected from sources other than the Data Subject, the information must be made available to the Data Subject within a reasonable time. If the personal data can be lawfully disclosed to another recipient, the Data Subject must be informed about it at the time of the first disclosure.

The obligation to provide information is not necessary if the Data Subject already has this information or if the recording or disclosure of personal data is expressly provided for by legislation or if the provision of information to the Data Subject proves impossible or required a disproportionately large effort.

The Data Subject must ensure that they receive access to their data processed by the Company free of charge, request their rectification or erasure, and exercise their right to object. The Data Controller is obliged to respond to the request of the Data Subject without undue delay, but no

later than within 25 (twenty-five) days, or if the Data Controller does not comply with any request of the Data Subject, it must justify it.

2.2 Purpose limitation principle

Personal data may only be collected for a specific, clear, and lawful purpose. It is prohibited to process personal data in a way that is incompatible with their purposes.

The processing of personal data for purposes other than the original purpose for which they were collected is permitted only if data processing is compatible with the original purposes for which the personal data were originally collected. In this respect, it is necessary to examine but not limited to, the relationship between the original and intended purposes of data processing, the circumstances of data collection and the nature of the personal data.

2.3 Principle of data minimisation

The processing of personal data must be appropriate and relevant for the purposes and the processing of personal data must be limited to the necessary minimum.

To ensure the implementation of the principle, the Data Controller must implement appropriate technical and organisational measures, such as pseudonymisation, both in determining how the data are processed and in the data processing process, with the aim of, firstly, implementing the data protection principles and, secondly, incorporating the guarantees necessary for the protection of the rights of the Data Subjects into the data processing process.

The Data Controller is obliged to implement technical and organisational measures that ensure that only personal data necessary for the specific purpose of data processing are processed. This obligation applies to the amount of personal data collected, the extent of their processing, the duration of their storage and their accessibility.

2.4 Principle of accuracy

The personal data collected, stored and processed by the Data Controller must be accurate and, if necessary, up to date. The Data Controller must take all reasonable measures to forthwith erase or rectify personal data that are inaccurate for data processing.

To ensure the implementation of the principle of accuracy, the Data Controller is obliged to verify the accuracy of the data (right to rectification and erasure) in the event of a request made to that effect by the Data Subject and, if necessary, to modify and erase the specified personal data.

2.5 Principle of storage limitation

To ensure the implementation of the purpose limitation principle, it must be ensured, in particular, that the period for which the personal data are stored is limited to a strict minimum. To ensure that the personal data are not kept longer than necessary, the Data Controller must set deadlines for erasure or for a perc review.

Personal data must be stored in such a way that the identification of the Data Subject can only be possible for the time necessary to achieve the purposes for which the personal data are

processed. Personal data may be stored for a longer period only if their processing is for archiving purposes in the public interest, for scientific and historical research, or statistical purposes.

2.6 Principle of integrity and confidentiality

Personal data must be processed in a manner that ensures their appropriate security and confidentiality, including preventing unauthorised access to or use of personal data and the equipment used for their processing.

To ensure the implementation of the principle, the Data Controller must use technical or organisational measures during the processing of personal data to ensure that the security of the personal data is satisfactory throughout. In this respect, it is necessary to also protect against the unauthorised or unlawful processing, accidental loss or destruction of or damage to the data.

2.7 Accountability of the Data Controller

The Data Controller is obliged to comply with the principles detailed above and to be able to prove compliance during the processing of personal data.

3. Rights of the Data Subject

3.1 Right of access

At the request of the Data Subject, the Data Controller provides information on whether their personal data are being processed; if so, it should grant access to the Data Subject.

3.2 Right to rectification

At the request of the Data Subject, the Data Controller corrects any inaccurate personal data relating to the Data Subject or supplements any incomplete data without undue delay.

3.3 Right to erasure

At the request of the Data Subject, the Data Controller erases the relevant personal data without undue delay if one of the following reasons exists:

- if the purpose of data processing has ceased to exist or if its statutory deadline has expired;
- if the Data Subject revokes their consent and there is no other legal basis for data processing;
- if the Data Subject objects to data processing and there is no priority legitimate reason for it;
- if the data processing is unlawful;
- if the personal data are incomplete or incorrect, and this condition cannot be remedied lawfully;
- it needs to be erased under the provisions of the legislation;
- if ordered by an authority or the court.

If the Data Controller has disclosed the personal data which it has to erase on the basis of the above, it is obliged to take all measures to inform the other Data Controllers of the obligation of erasure, as far as possible (state-of-the-art and implementation costs).

The personal data need not be erased even in the case of the above reasons for erasure if data processing is necessary for one of the following reasons:

- for exercising the right to freedom of expression and information;
- for compliance with a legal obligation which the Data Controller is subject to or performing a task in the public interest assigned to the Data Controller;
- no health data specified in legislation may be erased for the purpose of public interest in public health;
- for archiving in the public interest, for scientific and historical research purposes, or for statistical purposes, where erasure would be likely to render impossible or seriously jeopardise data processing;
- required for the submission and enforcement of legal claims or for indictment.

3.4 Right of restriction of processing

At the request of the Data Subject, the Data Controller restricts the processing of their personal data if one of the following conditions is fulfilled:

- the Data Subject disputes the accuracy of their personal data (in this case, the restriction applies to the period that allows the Data Controller to verify the accuracy of the personal data);
- the Data Controller no longer needs the personal data of the Data Subject, nonetheless, it requires them for submitting, enforcing or protecting legal claims;
- the Data Subject has objected to data processing; in this case, the restriction applies to the period that allows the Data Controller to examine whether the legitimate interests of the Data Controller take precedence over the legitimate reasons of the Data Subject.

During the restriction of data processing, it must be ensured that no data processing operation can be carried out on personal data. During the restriction of data processing, personal data may only be processed by the Data Controller, except for storage, with the consent of the Data Subject or for submitting, enforcing or protecting the legal claims of the Data Controller or for protecting the rights of other natural or legal persons or out of important public interest of the EU or a Member State.

In the event of a restriction of data processing, the Data Controller informs the Data Subject in advance of its lifting.

3.5 Right to object

The Data Subject is entitled to object at any time to the processing of their personal data by the Data Controller if its legal basis is the exercise of rights in the public interest or the prerogatives of public authority conferred on it or the enforcement of the legitimate interests of the Data Controller or a third party. The Data Subject may also exercise the right to object by automated means based on technical specifications by unsubscribing from the newsletter.

3.6 Right to data portability

The data subject is entitled to receive the personal data related to them and provided by them to a Data Controller in a structured, commonly used and machine-readable format and to transmit such data to another Data Controller without being hindered by the Data Controller to which it has provided the personal data.

3.7 Right of revocation

The Data Subject is entitled to revoke their consent to the processing of their personal data by the Data Controller at any time. The revocation of consent does not affect the lawfulness of data processing based on consent before such revocation. After the revocation of consent, the Data Controller is obliged to delete the personal data processed based on such consent.

3.8 Right of remedy of the Data Subject

In the event of a complaint about data processing, if you have any requests or questions about data processing, you can send your inquiry by post to the registered office of the Data Controller or electronically to the e-mail address indicated in the contact details of the Data Controller. We will send our answers without delay, but within no more than 15 (fifteen) days to the address you requested.

The Data Subject is entitled to lodge a complaint to:

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

A judicial remedy is available against the decision of the supervisory authority.

The Data Subject is entitled to initiate proceedings with the court to remedy the infringement sustained if the Data Controller does not process their personal data by legislation. The Data Controller is obliged to compensate the Data Subject for pecuniary and non-pecuniary damages caused by unlawful data processing. The adjudication of data protection lawsuits falls within the competence of the regional court. The Data Subject may also file a lawsuit, at their option, before the regional court with jurisdiction at their domicile of residence.

3.9 Data processors

	Name	**Registered office**	**E-mail**	**Responsibilities**
E-mail provider	Microsoft Outlook	USA, Washington State, Seatle –	www.support.microsoft.com/hu-hu/contactus	We will notify the registrants and will

		Redmond One Microsoft Way		keep in touch with them through it.
Storage	Hubspot	London Address Knotel, Floor 4, Clerks Court 18-20 Farringdon Lane, London EC1R 3AU	https://www.hubspot.com/company/contact	Website Domains are stored here.
Newsletter	MailChimp	The Rocket Science Group, LLC 675 Ponce de Leon Ave NE Suite 5000 Atlanta, GA 30308 USA	https://mailchimp.com/contact/	Registrants will receive newsletters through it.
Email Marketing	Hubspot	London Address Knotel, Floor 4, Clerks Court 18-20 Farringdon Lane, London EC1R 3AU	https://www.hubspot.com/company/contact	Registrants will receive marketing emails through it.
Workspace	Google workspace	1600 Amphitheatre Parkway, Mountain View, California USA	https://www.google.com/contactus	Help to work with the registrants

4. Data protection officer and their contact details

Under Article 37 of GDPR, the Data Controller is not obliged to appoint a data protection officer.

5. Process of data processing

The data may be processed by the staff of the Data Controller only to the extent essential for performing their tasks if the Data Controller employs staff. If it does not employ any staff, the data will be processed by the representative of the Data Controller.

Please note that the Data Controller does not perform any data processing activity in connection with the functions invited by the shortcuts of external service providers (Facebook, Twitter, LinkedIn and Instagram) appearing on the website. In these cases, the data controller is the third-party company providing the service.

5.1 Data processed during the use of the Website

Data processed:	***NAME***
It is mandatory to provide:	mandatory
Purpose of data processing (what are the data needed for):	registration, identification
Legal basis for data processing:	in the case of registration performance of the contract, Article 6(1)(b) GDPR, or consent of the Data Subject, Article 6(1)(a) GDPR in the case of a newsletter, consent of the Data Subject, Article 6(1)(a) GDPR, and statutory requirement, Article 6(1)(c) GDPR
Who can see the data:	authorised staff of the Data Controller and authorised staff of the Data Processors
Duration of data processing:	until registration is cancelled, or at the latest until the concluded contracts are fulfilled, or until unsubscribing from the newsletter
How can the data be deleted:	in the case of registration by deleting the registration in a message to the data controller (in case of teams before selection) in the case of a newsletter, revoking consent by using the unsubscribe link in the newsletter

Data processed:	***E-MAIL ADDRESS***
It is mandatory to provide:	mandatory
Purpose of data processing (what are the data needed for):	registration, identification
Legal basis for data processing:	in the case of registration performance of the contract, Article 6(1)(b) GDPR, or consent of the Data Subject, Article 6(1)(a) GDPR in the case of a newsletter, consent of the Data Subject, Article 6(1)(a) GDPR, and statutory requirement, Article 6(1)(c) GDPR
Who can see the data:	authorised staff of the Data Controller and authorised staff of the Data Processors

Duration of data processing:	until registration is cancelled, or at the latest until the concluded contracts are fulfilled, or until unsubscribing from the newsletter
How can the data be deleted:	in the case of registration by deleting the registration in a message to the data controller (in case of teams before selection) in the case of a newsletter, revoking consent by using the unsubscribe link in the newsletter

Data processed:	***PROJECT NAME***
It is mandatory to provide:	mandatory
Purpose of data processing (what are the data needed for):	identification
Legal basis for data processing:	performance of the contract, Article 6(1)(b) GDPR,
Who can see the data:	authorised staff of the Data Controller and authorised staff of the Data Processors
Duration of data processing:	until registration is cancelled, or at the latest until the concluded contracts are fulfilled
How can the data be deleted:	in the case of registration by deleting the registration in a message to the data controller (in case of teams before selection)

Data processed:	***DATA AND COMPETENCES OF REGISTRANT***
It is mandatory to provide:	mandatory
Purpose of data processing (what are the data needed for):	identification
Legal basis for data processing:	performance of the contract, Article 6(1)(b) GDPR,
Who can see the data:	authorised staff of the Data Controller and authorised staff of the Data Processors
Duration of data processing:	until registration is cancelled, or at the latest until the concluded contracts are fulfilled
How can the data be deleted:	in the case of registration by deleting the registration in a message to the data controller (in case of teams before selection)

Data processed:	***PROJECT INFORMATION***
It is mandatory to provide:	mandatory
Purpose of data processing (what are the data needed for):	identification
Legal basis for data processing:	performance of the contract, Article 6(1)(b) GDPR,
Who can see the data:	authorised staff of the Data Controller and authorised staff of the Data Processors
Duration of data processing:	until registration is cancelled, or at the latest until the concluded contracts are fulfilled
How can the data be deleted:	in the case of registration by deleting the registration in a message to the data controller (in case of teams before selection)

5.2 Complaints management

Complaining is based on voluntary consent, but under the data processing legislation (article 6 paragraph 1 letter b) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons about the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) it is mandatory in respect of the processed data.

Name, description and purpose of data processing	**Complaints management** You may report your complaint about the service or product or the conduct, acts or omissions of the Data Controller in writing (by post or e-mail). The purpose of data processing is to identify the Data Subject and the complaint as well as to record the data that are mandatory to be recorded from the law, as well as to enable the communication of the complaint and to maintain contact.	
Scope of Data Subjects	Every natural person who wishes to report a complaint about the service or the conduct, acts or omissions of the Data Controller in writing.	
Legal basis for data processing	The complaint-handling process starts based on voluntary consent, but in the case of a complaint, it is mandatory under the legislation on data processing.	
Scope and purpose of the processed data	Complaint ID	identification
	Place, time and manner of receipt of the complaint	identification
	E-mail address	identification, liaison
	Personal data provided by e-mail	identification

	Last name	identification
	First name	identification
	Mailing address	liaison
	Subject-matter of complaint	complaints management
	Content of complaint	investigation of complaint
	Attached documents	investigation of complaint
	Reason for complaint	investigation of complaint
Duration of data processing and erasure of data	The Data Controller retains the record of the complaint and a copy of the response for 5 years from their date pursuant.	
Who can have access to personal data?	● authorised staff of the Data Controller	
	● authorised staff of the Data Processor	
Method of data storage	electronic	

5.3 Request for information

The request for information is based on voluntary consent and the forms previously submitted by the applicants.

Name, description and purpose of data processing	**Request of information** You can ask questions about the service or the conduct and activities of the Data Controller in writing (by post or e-mail). The purpose of data processing is to provide the Data Subject with appropriate information and to maintain contact.	
Scope of Data Subjects	Any natural person who contacts the Data Controller and requests information from the Data Controller in addition to providing their personal data.	
Legal basis for data processing	In accordance with the purpose of data processing, you voluntarily consent to the Data Controller contacting you through such data to clarify or answer the question if you provided your contact details when the information was requested.	
Scope and purpose of the processed data	Question ID	identification
	Place, time and manner of receipt of the question	identification
	E-mail address	identification, liaison
	Personal information provided by e-mail	identification
	Last name	identification
	First name	identification
	Mailing address	liaison
	Subject-matter of question	complaints management
	Business related questions	research
	Content of question	investigation of complaint
Duration of data processing and erasure of data	Until the goal is achieved.	

Who can have access to personal data?	● authorised staff of the Data Controller ● authorised staff of the Data Processor
Method of data storage	electronic

5.4 Additional information

Some of your data, as shown in the table, are also visible to our other users (recipients) to whom you have made them visible. However, this does not constitute either data transmission or data transfer. Other users can only see your data but may not perform data processing activities other than viewing them, so you may not process third-party data either besides viewing them unless they have specifically consented to it, but this is your legal relationship independent of the Data Controller.

By entering the mandatory data and ticking the checkbox, you consent to it being visible to other users according to 'visibility settings' and to the Data Controller processing them for the purpose indicated in the above table.

By entering the data to be provided voluntarily, optionally, you consent to it being visible to other users according to the 'visibility settings' and to the Data Controller processing them for the purpose and time indicated in the above table. It is not necessary to tick the checkbox here, it only needs to be done at the time of registration, while these data can be provided after registration.

The Data Controller is responsible for ensuring that the data are up to date and accurate, so we ask you to notify the Company forthwith of any changes in the data.

5.5 Sharing data

Company reserves the right to share every data and information with the partners enlisted in the Privacy Notice.

6. Data security

The Data Controller provides data security. To this end, it takes the technical and organisational measures and establishes the rules of procedure that are required for the enforcement of the governing legislation and rules of data protection and confidentiality.

The Data Controller protects, through appropriate measures, the data against unauthorised access, alteration, transmission, disclosure, erasure or destruction, and accidental destruction and damage as well as becoming inaccessible because of a change in the technology applied.

The Data Controller (also) ensures the enforcement of the data security rules using internal regulations, instructions and rules of procedure separate from the Data Protection and Data Security Regulations and this Notice in content and form.

When specifying and applying measures aimed at data security, the Data Controller takes into consideration the current development level of technology and chooses a data processing

solution from several alternatives which provides a higher level of protection of personal data unless it would represent disproportionate difficulties.

Within the scope of its tasks related to IT protection, the Data Controller provide, in particular, for:

- measures to protect against unauthorised access, including the protection of software tools and hardware devices and physical protection (access protection, network protection);
- measures to ensure the possibility of restoring data files, including regular backups and the separate, secure processing of copies (mirroring, backup);
- the protection of data files against viruses (virus protection);
- the physical protection of data files and the devices carrying them, including protection against fire, water damage, lightning, and other natural forces, and the recoverability of damage resulting from such events (archiving, fire protection).

The Data Controller ensures the proper backup of the IT data and the technical environment of the Website, which it operates with the necessary parameters based on the retention period of each data, thus guaranteeing the availability of the data within the retention period and will permanently destroy them upon the expiration of the retention period.

It monitors the integrity and functionality of the IT system and the data storage environment with advanced monitoring techniques and continuously provides the necessary capacities. It records events in its IT environment using complex logging functions, thus ensuring the subsequent detectability and legal proof of possible incidents.

We are constantly using a redundant network environment that provides high bandwidth to serve the Website, which securely distributes the loads that occur between our resources.

We guarantee the disaster resilience of our systems as planned and ensure business continuity and thus the continuous service of our users at a high level with organisational and technical means.

With a high priority, we ensure the controlled installation of security patches and manufacturer upgrades that also ensure the integrity of our IT systems, thus preventing, avoiding and managing attempts to access or damage them by exploiting vulnerabilities.

We regularly inspect our IT environment with security testing, correct any errors or weaknesses found, and consider strengthening the security of the IT system to be an ongoing task.

We have formulated high-security requirements for our employees, including confidentiality. We also ensure that they are met through regular training, and in connection with our internal operations, we strive to operate planned and controlled processes.

Any incidents involving personal data, which are detected by or reported to us during our operations will be investigated transparently, by responsible and strict principles, within 72 hours. Incidents that have occurred are handled and recorded.

During the development of our services and IT solutions, we ensure the fulfilment of the principle of built-in data protection. We treat data protection as a priority requirement already in the planning phase.

7. Data transmission

The Data Controller is entitled to transmit the personal data collected, recorded, and organised by it to a third party.

The principles of data processing (for example, the principle of data minimisation, and the purpose limitation principle) must be observed throughout the data transmission. During data transmission, it must also be borne in mind that the recipients should also ensure an appropriate level of protection for the personal data of the Data Subject.

The Data Controller may only use a Data Processor who or which provides appropriate guarantees for the requirements set out in the General Data Protection Regulation and implements appropriate technical and organisational measures, which ensure the protection of Data Subjects. The Data Processor is only entitled to transmit personal data if instructed to do so by the Data Controller. Where the obligation to transmit data is required by the law of a Member State under the law of the Data Processor or by the EU law applicable to it, the transmission may take place without the instructions of the Data Controller, but with its prior notification.

8. Amendment of the Notice

The Company reserves the right to amend this Notice at any time by unilateral decision.

If the Data Subject does not agree with the amendment, they may request the erasure of their personal data via contacting the Company.

Any questions and reservations concerning this Privacy Policy should be sent to the Company.