
Privacy Policy
of SpeedUp Venture Capital Group
with its registered office in Poland, Poznań, ul. Św. Marcin 11/8, e-mail: gdpr@speedupgroup.com

Maintaining the confidentiality of your data is extremely important to us and we want you to know how we process it. For this reason, and in order to fulfil the legal obligations arising from the GDPR, we have drawn up a Privacy Policy that describes the way personal data is protected and processed at SpeedUp Venture Capital Group.

Remember that within the meaning of the GDPR, personal data is any information concerning an identified or identifiable natural person ("data subject"). In turn, an identifiable natural person is a person who can be directly or indirectly identified, in particular on the basis of an identifier such as name, identification number, location data, internet identifier or one or more specific factors determining physical, physiological, genetic, psychological, economic, cultural or social identity of a natural person. Importantly, data concerning legal persons is not covered by the regulations arising from the GDPR.

By entering into relationships with each of the SpeedUp Venture Capital Group entities (hereinafter referred to as the "SpeedUp Group"), including in particular submitting investment proposals to us or participating in our acceleration programs, you entrust us with your personal data. The cooperation between entities of the SpeedUp Group aims at, among others, ensuring the best possible business analysis of your investment, and subsequently – if we decide to invest in it – its handling.



This privacy policy was published on 1. Aug. 2024. and applies to all Users of the www.speedupgroup.com website (hereinafter referred to as the Website), as well as users of the forms available there (subscription to the newsletter), all users of our social media accounts (Facebook, Twitter, LinkedIn), and all persons submitting investment proposals or contacting us in other matters.

We forbid people under the age of 18 to use the website without the consent of a parent or an adult guardian. We do not knowingly collect personal information from children under the age of 13.

We reserve the right to make amendments to this Policy ([more](#))

Previous versions: none

Effective as of: 1. Aug. 2024.

Table of contents

1. Who is responsible for your personal data?	2
A. If you subscribe to the Speed Up Group newsletter:	2
B. In other cases:	2
2. Joint arrangements between the Controllers.	2
3. How do we collect your data?	3
4. Your rights related to the processing of personal data.	3
5. What happens to your data when:	8
A. you submit an investment offer to us:	8
B. you apply for programs organised by us, e.g. acceleration ones:	10



C. you contact us in other matters:	10
D. you subscribe to our newsletter:	11
E. you use our website www.hugething.vc :	12
F. you click on social media plugins located on our Website or use our social media accounts:	13
6. Changes to the Privacy Policy.	14

§1. Who is responsible for your personal data?

A. If you subscribe to the Speed Up Group newsletter:

The controller of your data is Speedup Management sp. z o.o with its registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, entered into the Register of Entrepreneurs of the National Court Register under the number KRS 0000265669, NIP 7781440558, REGON 30043371200000, e-mail: gdpr@speedupgroup.com.

B. In other cases:

i.e. when you browse our website www.speedupgroup.com, use our social media accounts (Facebook, Twitter, LinkedIn), contact us, including submitting investment offers:

The controller of your personal data are the entities included in the SpeedUp Venture Capital Group with its registered office in Poznań, Poland, which jointly control the data, jointly deciding on the purposes and methods of its processing.

Our contact details: SpeedUp Venture Capital Group CONTACT POINT, ul. Św. Marcin 11/8, 61-803 Poznań, Poland, e-mail: gdpr@speedupgroup.com

IMPORTANT! Despite the designation of the Contact Point, you are entitled to exercise your rights towards each of the Joint Controllers. In such a case, your request will be forwarded by the Joint Controller to Speedup Management sp. z o.o., which will respond to the request.

Personal Data Protection Inspector.

In order to protect personal data, we have appointed a Data Protection Officer at Ms Monika Synoradzka, who is contacted by e-mail at GDPR@speedupgroup.com or by phone at +48 61 671 01 71, or by correspondence: ul. SW. Marcin 11/8, 61-803 Poznań, Poland.

SpeedUp Venture Capital Group consists of the following entities:

1. Speedup Management sp. z o.o. company with its registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, KRS 0000265669, NIP 7781440558, REGON 30043371200000;
2. HUGE THING sp. z o.o. company with registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, KRS 0000411691, NIP 9721238305, REGON 30205504200000;
3. SpeedUp Innovation sp. z o.o. sp. k-a company with its registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, KRS 0000433149, NIP 7831691921, REGON 30221022900000;
4. Speedup Bridge Alfa sp. z o.o. company with its registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, KRS 0000552776, NIP 9721254008, REGON 36096349000000;
5. SEEDSTONE SPEEDUP MANAGEMENT SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ ASI SPÓŁKA KOMANDYTOWO-AKCYJNA company with its registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, KRS 0000478561, NIP 7831704954, REGON 30255661400000;



6. HT Inwestycje Spółka z ograniczoną odpowiedzialnością z siedzibą company with its registered office in (61-803 Poznań) at ul. Św. Marcin 11/8, KRS 0000861071, NIP 7831824724, REGON 387116151,

hereinafter referred to as the Joint Controllers.

Relevant information about joint control can be found right below in clause 2.

§2 Joint arrangements between the Controllers.

Due to the fact that the SpeedUp Group operates on the basis of joint control, your Personal Data is jointly controlled by entities included in the SpeedUp Group with its registered office in Poznań – you can find a list of these entities [here](#). In other words, within the SpeedUp Group, we jointly decide on the purposes and methods of processing of the data that we possess.

In view of the above, we have decided to conclude an agreement on the joint control of data. Thanks to this, it is possible to create a coherent system of personal data protection for all Joint Controllers.

The provisions of the joint control agreement concluded by us, which are relevant to you, can be found below:

1. Your personal data is **JOINTLY CONTROLLED** by entities included in the SpeedUp Group for the purposes of: developing the "SpeedUp Venture Capital Group" brand by creating an opportunity to comprehensively provide services at the highest level possible, using innovative solutions and with the help of staff that possesses appropriate skills and qualifications, including striving for unified customer service and reducing operating costs through synergy – on the basis of the Agreement on joint control of data.
2. An extract from the provisions of the agreement on joint control of data, which are relevant to you, is available upon request. Here, we indicate that:
 - a) the entity responsible for the fulfilment of the information obligation towards you is Speedup Management sp. z o.o.,
 - b) the entity responsible for answering your inquiries and exercising your rights is Speedup Management sp. z o.o.,
 - c) we have not appointed a Personal Data Protection Officer,
 - d) we have established the following CONTACT POINT for natural persons, whose personal data is jointly controlled by us: SpeedUp Venture Capital Group CONTACT POINT, ul. Św. Marcin 11/8, 61-803 Poznań, Poland, e-mail: gdpr@speedupgroup.com

IMPORTANT! Despite the designation of the Contact Point, you are entitled to exercise your rights towards each of the Joint Controllers. In such a case, your request will be forwarded by the Joint Controller to Speedup Management sp. z o.o., which will respond to the request.

Personal Data Protection Inspector. In order to protect personal data, we have appointed a Data Protection Officer at Ms Monika Synoradzka, who is contacted by e-mail at GDPR@speedupgroup.com or by phone at +48 61 671 01 71, or by correspondence: ul. SW. Marcin 11/8, 61-803 Poznań, Poland.

Each of the Controllers exercises due diligence in order to ensure the security of the processing of your data, and you can contact each of them in case you have any questions.

§3 How do we collect your data?

Some data is collected when you share it with us. This may be, for example, data provided to us in the e-mail correspondence addressed to us or investment proposals submitted, registration data provided when



subscribing to the newsletter or data provided when concluding a contract with us. As well it may also be your personal data, that you provide to us by sending your CV when we are not recruiting.

Other data is collected automatically by our IT systems when visiting our Website. This is data collected by the cookies used on our website. You can read about it in a separate document, i.e. our [Cookies policy](#).

§4 Your rights related to the processing of personal data.

SpeedUp Venture Capital Group CONTACT POINT, ul. Św. Marcin 11/8, 61-803 Poznań, Poland, e-mail: gdpr@speedupgroup.com

IMPORTANT! Despite the designation of the Contact Point, you are entitled to exercise your rights towards each of the Joint Controllers. In such a case, your request will be forwarded by the Joint Controller to Speedup Management sp. z o.o., which will respond to the request.

1. Each data subject is entitled to submit a request to us in order to exercise the rights referred to in art. 15 – 22 of the GDPR, i.e.:
 - A. the right of access to data,
 - B. the right of rectification of data,
 - C. the right to erasure ("the right to be forgotten"),
 - D. the right to restrict processing,
 - E. the right to data portability,
 - F. the right to object to the processing of personal data,
 - G. the right to not be a subject to automated decision-making in individual cases, including profiling,
You can object to such processing at any time.
Currently, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data.
 - H. the right of withdrawal,
Withdrawal of consent will not affect the lawfulness of the processing we have carried out on the basis of consent expressed prior to its withdrawal.
 - I. the right to lodge a complaint with a supervisory authority.
You can lodge a complaint with the supervisory authority, both in Poland (the President of the Personal Data Protection Office, helpline: 606 950 000), and in the EU Member State of your habitual residence, place of work or alleged violation.
2. Requests may be submitted:
 - a) by post to the following address: SpeedUp Venture Capital Group CONTACT POINT, ul. Św. Marcin 11/8, 61-803 Poznań, Poland;
 - b) electronically to the e-mail address: gdpr@speedupgroup.com
 - c) in person at our headquarters, i.e. at ul. Św. Marcin 11/8, 61-803 Poznań, Poland;
3. We consider the requests of data subjects with due diligence, taking into account the provisions of law as well as the rights and freedoms of other data subjects.
4. When submitting your request, you should provide data that allows for your unambiguous identification.
5. We do not refuse to take action at the request of the data subject wishing to exercise their rights unless we are unable to unambiguously identify the data subject.
6. We provide information about the actions taken in connection with the request without undue delay – or in any case within one month of receiving the request. If necessary, we may extend this time limit by another



two months due to the complex nature of a request or the number of requests. Within one month of receiving the request, we will inform you of such an extension of time limit, providing the reasons for the delay.

7. If we receive your request electronically, we will provide the response electronically as well, if possible, unless you request otherwise.
8. If we do not take action in connection with your request, we will immediately inform – at the latest within one month of receiving the request – about the reasons for not taking action and about the possibility of lodging a complaint to the supervisory body and using judicial remedies.
9. Communication and actions taken in connection with exercising your rights are, as a rule, free of charge. However, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character, we may:
 - a) collect a reasonable fee, taking into account the administrative costs of providing information, carrying out communication or undertaking the required actions; or
 - b) refuse to undertake action in relation to the request.
10. If we cannot unambiguously identify you or if we have reasonable doubts in regard to your identity, we may request additional information necessary to confirm your identity. If you do not provide additional information within 30 days from the date of receiving the request to do so, and your unambiguous identification is impossible, the application will be rejected. You will be informed about the deadline for providing additional data and the consequences of not providing them.
11. We inform every recipient to which we have disclosed your personal data about its rectification, completion, erasure or restriction of its processing, unless it would prove to be impossible or require a disproportionate effort.

More details about your rights you can find below..

A. The right of access by the data subject.

1. You have the right to obtain information from us as to whether we process your data. If so, you have the right to access your data and obtain information including:
 - a) the purposes of the processing,
 - b) categories of collected data,
 - c) specification of recipients, to which the data will or have been disclosed,
 - d) the planned period of data storage or the criteria for determining this period,
 - e) an indication of your rights, i.e. the right to rectify data, erase data or restrict its processing, the right to object to the processing, the right to lodge a complaint with the supervisory authority,
 - f) data sources, if the data comes from a source other than the data subject,
 - g) information about the existence of automated decision-making, including profiling, as well as the importance and anticipated consequences of such processing for the data subject,
 - h) information on appropriate safeguards related to the transfer of data if it is transferred to a third country or an international organisation.
2. We can provide you with a copy of your personal data that we possess. The first copy of the data is free of charge. For each subsequent copy of the data, we may charge a fee in the amount based on administrative costs.
3. If you request a copy electronically – we provide information via common electronic means to the e-mail address, from which the inquiry came. You can request a copy provided via other means.
4. If we process large amounts of information about you – we may first ask you to indicate what specific information you seek.



B. The right to rectification of data.

1. You may request immediate rectification of your data – if the data is incorrect.
2. You may request the completion of data – if the data is incomplete.
3. We inform each recipient, to which this personal data has been disclosed, about the rectification of your data, unless this proves impossible or involves a disproportionate effort.

C. Right to erasure ("right to be forgotten").

1. You have the right to request the erasure of your personal data if:
 - a) we no longer need the personal data for the purpose for which it was collected or processed in any other way,
 - b) the basis for processing was your consent and you have withdrawn this consent (and we no longer have any other legal basis for the processing of your data),
 - c) you have objected to the automated decision-making in your individual cases, including profiling,
 - d) personal data have been unlawfully processed by us,
 - e) we must erase personal data in order to comply with a legal obligation to which we are subject,
2. If your personal data has been made public by us – we will take measures in order to inform the entities, with which we have shared the data, about your request. These actions will be aimed at removing all links to this data and its copies. We will take these actions to the extent that the technology allows us to do so and taking into account the costs of carrying out these actions.
3. Your request will be processed immediately, unless further processing is necessary:
 - a) for exercising the right of freedom of expression and information,
 - b) for us to fulfil our legal obligation,
 - c) for reasons of public interest in the field of public health,
 - d) for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, provided that it is probable that the exercise of the right to erasure will prevent or seriously impair the fulfilment of the purposes of such processing,
 - e) for the establishment, exercise or defence of legal claims.

D. The right to restrict processing.

1. You have the right to request restriction of the processing of your data if:
 - a) you question the correctness of your personal data (then we will restrict the processing until the correctness of your data is verified),
 - b) we process data unlawfully, but despite that you object to its erasure and, in return, request the restriction of its use,
 - c) we no longer need your data, but you need it in order to establish, exercise or defend legal claims,
 - d) you have objected to the processing – until we determine whose rights are superior towards the processing being carried out – ours or yours;
2. If we restrict the processing, we may process your data (but with the exception of storage):
 - only with your consent,
 - to establish, exercise, or defend legal claims.
 - to protect the rights of another natural or legal person,
 - for reasons of important public interest of the European Union or a Member State.
3. Before revoking the processing restriction, we will inform you about it.
4. We inform each entity to which we disclosed your data about the restriction of data processing. We do it as far as possible, taking into account the effort we have to put into it.



E. The right to data portability.

The fulfilment of this request does not free us from the obligation to exercise other rights you have.

If you store the transferred data in your own IT or other type of system – you are responsible for taking appropriate measures in order to secure this data.

1. You have the right to request the transfer of your data.
2. This means that you have the right to receive this data:
 - in a structured, commonly used format
 - that is machine-readable.
3. However, this only applies to the data provided to us by you.
4. You have the right to send this personal data to another controller without any obstacles on our part if:
 - a) We process this data on the basis of consent or on the basis of a contract and
 - b) The processing is carried out by us in an automated manner.
5. You have the right to request that this data was sent by us directly to another controller. We will fulfil this request if it is technically possible.
6. The exercise of the right to data portability does not preclude you from submitting a request to erase your personal data.
7. The right to data portability does not apply to processing that is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in us.

F. The right to object.

It applies to processing carried out on the basis of our legitimate interest as well as automated processing consisting in making decisions in individual cases, including profiling, and processing for purposes of direct marketing.

1. You have the right to object if we process your data:
 - a) in the public interest,
 - b) in the exercise of official authority
 - c) on the basis of our legitimate interest,
 - d) or it is subject to profilingand there occurs a particular situation that justifies the objection.
 - In such case, you can object at any time.
 - When we receive the objection, we will stop processing your personal data.
 - We can only process the data further if we prove the existence of important and compelling legitimate grounds for processing that override your interests, rights and freedoms, or this data constitutes the basis for establishing, exercising or defending legal claims.
2. You also have the right to object if your personal data is being processed for purposes of direct marketing.
 - In such case, you can object at any time.
 - When we receive the objection, we will stop processing your data for purposes of direct marketing. We will fulfil this obligation with no additional exceptions. Therefore, there is no need for any particular situation to occur in order for your request to be fulfilled.
 - Note that despite such objection, your data may still be processed for other purposes.
3. You also have the right to object if we process your data for purposes of scientific or historical research or for statistical purposes.



- In this case, you can raise an objection if there occurs a particular situation that justifies such objection.
- We will not consider the objection if the processing is necessary for us to perform a task carried out in the public interest.

4. The right to not be a subject to automated decision-making in individual cases, including profiling.
You can object to such processing at any time.

Currently, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data.

G. The right not to be subject to a decision that is based solely on automated processing, including profiling, and entails legal implications for you or similarly significantly affects you.

- I. This right does not apply to situations where such processing:
 - a) is necessary for the conclusion or performance of a contract between us and you;
 - b) is authorised by the law to which we are subject, and this law lays down suitable measures to safeguard your rights, freedoms and legitimate interests or
 - c) is based on your explicit consent.
- II. If we will profile your data as part of automated decision-making, you have the right to object to such processing at any time – for reasons related to your particular situation.
- III. In the event of an objection, we will cease to process this personal data, unless we demonstrate the existence of compelling legitimate grounds for processing that override your interests, rights and freedoms, or we need this data to establish, exercise or defend legal claims.
- IV. If, as part of automated decision-making, your personal data is processed for purposes of direct marketing – you have the right to object at any time to the processing of your data for the purposes of such marketing, including profiling.
- V. In the event the data subject objects to the processing for purposes of direct marketing, we may no longer process the personal data for such purposes.

H. The right of withdrawal.

Withdrawal of consent will not affect the lawfulness of the processing we have carried out on the basis of consent expressed prior to its withdrawal.

1. If we process your data on the basis of your consent – you have the right to withdraw your consent at any time.
2. It is important to know that: Withdrawal of consent does not affect the lawfulness of the processing we have carried out on the basis of consent expressed prior to its withdrawal.

I. The right to lodge a complaint with a supervisory authority.

You can lodge a complaint with the supervisory authority, both in Poland (the President of the Personal Data Protection Office, helpline: 606 950 000), and in the EU Member State of your habitual residence, place of work or alleged violation.

1. If, in your opinion, we process your personal data unlawfully, you can lodge a complaint with the supervisory authority. The supervisory authority for us is the President of the Personal Data Protection Office: www.uodo.gov.pl, helpline: 606 950- 000. You can also lodge the complaint in the Member State of your habitual residence, place of work or place of the alleged violation.



§5 What happens to your data when:

A. you submit an investment offer to us:

The investment proposal that we receive is registered in our CRM program for managing and analysing such proposals. The data provided is analysed by our analysts (this mainly includes data concerning the team, product characteristics, target market, investment offer). At this stage, it may be necessary to consult the proposal with external experts – in that case we ask for your consent to transfer your data to such experts. Next, another analysis of the data provided is performed, which includes an analysis of the shareholding structure, competitive advantage, structure and dynamics of revenue, technology description, target market characteristics, team history, sales strategy, etc.). During analyses, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data. In the meantime, we conduct talks or meetings with you and inform you about the need to receive additional data – its provision is voluntary, but necessary to continue the process. Failure to provide this data results in the refusal to make the investment. The analysis ends with our decision to conduct further talks aimed at making the investment, or to thank you for the investment. If we and you decide to take further steps aimed at making the investment, then we sign a document called the Term Sheet. Along with the Term Sheet, we will provide you with further information on the processing of the data provided to us, as this process will depend on our arrangements in this regard.

What kind of personal data do we process?

We process the data you provide to us – these are mainly your contact details, such as: e-mail address, phone number, LinkedIn identifier, sometimes a photo (if it is part of the message sent to us). Along with the investment offer submitted to us, we process a number of data related to this offer. This includes data of public nature (company name, its short description) as well as private information (business plan, executive summary, financial plan, achievements, plan for the future, description of the idea).

On what basis and for what purposes do we process your data?

Your data is processed:

- in order to contact you, respond to the submitted offer and exchange further correspondence regarding the offer – based on your consent and in connection with activities aimed at concluding an agreement;

You have the right to withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of the processing we have carried out on the basis of consent expressed prior to its withdrawal.

- in order to take steps aimed at concluding an investment agreement and if we decide to do so – also for the purpose of the conclusion of an investment agreement – based on your interest in our services and actions taken by you that aim at concluding an agreement;
- in order to enable a quick and efficient evaluation of your subsequent investment offers submitted to us, based on already made analyses on the basis of previously provided data – based on our legitimate interest – balancing test available upon your request. You have the right to object to such processing of your data.
- for evidence purposes, to secure information in the event of a legal need to prove facts and to establish, exercise or defend against legal claims – based on our legitimate interest – balancing test available upon your request. You have the right to object to such processing of your data.

Who do we share your data with – data recipients?

We share your data with:

- entities belonging to the SpeedUp Group, based on the Agreement on the joint control of data – the current list of entities belonging to the SpeedUp Group is available upon request.



- subcontractors, i.e. entities we use during the processing of data, with which we have concluded a contract for entrusting the processing of personal data, including: our hosting service provider, our CRM software provider, entities providing IT support services to us, including:
 - ▣ provider of the Google Workspace software pack for companies, including e-mail, i.e. Google LLC, whose registered office is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA;
 - ▣ provider of project management software called "ASANA", i.e. Asana Inc., whose registered office is located at 1550 Bryant Street, Suite 200, San Francisco, CA 94103.
- offices, state authorities and administrative bodies to the extent required by law.

A detailed list of data recipients is available upon your request.

Do we transfer your data outside the European Economic Area, and on what basis?

Be advised that we transfer your data outside the European Economic Area, but these solutions guarantee the legally required level of data security:

- in connection with the use of cookies on our website – read more in the Cookies Policy;
- in connection with the use of the software pack of Google services for companies, including e-mail, where the registered office of Google LLC is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.
- in connection with the use of project management software called "ASANA" provided by Asana Inc., whose registered office is located at 1550 Bryant Street, Suite 200, San Francisco, CA 94103.

Thus, your data may be transferred to the United States of America (USA) or other countries outside the European Union, where these companies' servers are located, to the extent of their storage on these servers. In this case, the recipient of your data in the aforementioned third country will be Google LLC or Asana Inc., respectively, to whom we entrusted the processing of your personal data as a processor.

We provide adequate security for your personal data using standard data protection clauses approved by the European Commission and under which certain basic guarantees of the security of your data have been established. Well, all Google and Asana services have built-in advanced security features that constantly protect your data and allow you to detect and automatically block potential security threats. The data is protected against unauthorized access, modification, disclosure, or destruction. Security measures include, but are not limited to encryption to ensure data privacy while in transit; a range of security features, such as safe browsing, security checking, and two-step verification of data access; controlling the procedures for collecting, storing, and processing information, including physical security measures to prevent unauthorized access to Google or Asana systems. Access to personal data is restricted. Only Google or Asana reps who need them in order to process them have it. Any person having such access is obliged to maintain strict confidentiality, and in the event of failure to comply with these obligations, may suffer consequences, including termination of cooperation.

You can find out more about the security of your data in connection with our use of Google's business suite of applications here:

https://workspace.google.pl/intl/pl/security/?secure-by-design_activeEl=data-centers

You can find more about the security of your data in connection with our use of ASANA software here:

<https://asana.com/security-statement>

At any time, you have the right to obtain a copy of your personal data transferred to a third country, a copy of contractual clauses, a shortened description of security measures, and a copy of any contract regarding the data subcontracting service.

How long do we process your personal data?



- always for the period necessary to fulfil the purposes of processing, but no longer than until the consent is withdrawn or an objection is raised;
- we process the data obtained for the purpose of providing a response for the period necessary to provide the response/clarify the matter or until you withdraw your consent to data processing, or we determine that the data has become obsolete,
- we store the data provided to us in order to conclude an investment agreement for 10 years since the decision to submit an investment offer or to refuse to submit it – the period of 10 years is a period corresponding to the economic cycle in which you return to us with further investment offers, and having analyses of the previously provided data allows for faster and more efficient evaluation of your new investment offers.

How do we profile and target your data?

Currently, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data.

Is the provision of data obligatory or voluntary?

To the extent that data is processed in order to contact you or respond to questions, or to analyse your investment offer – providing data is voluntary. The consequence of not providing data will be the inability to make contact/ respond/ analyse investment offer.

For the conclusion and performance of a contract, we collect only the data without which the contract cannot be performed. Failure to provide the data necessary to conclude and perform the contract will result in us not being able to conclude it with you or perform it. This also applies to data that we must collect due to our legal obligations (e.g. data for invoices).

The consent to the processing of personal data is voluntary. If you do not give us the consent that we ask for, then we will not take the actions to which that consent applies. You may withdraw your consent at any time.

NOTE! Withdrawal of consent, however, does not affect the lawfulness of the processing of your personal data done by us, which we have carried out on the basis of consent expressed prior to its withdrawal.

B. you apply for programs organised by us, e.g. acceleration ones:

This Policy does not apply to the processing of data that you provide to us as part of applying to participate in programs organised by us, e.g. acceleration ones. The rules for the processing of your data in connection with applying are described in the regulations of such programs or in other documents that you read before deciding to apply. These rules may differ from those described below, in particular in terms of the group of entities that have access to your data, the purposes of processing and the methods of its processing.

C. you send us your CV when we are not recruiting**What kind of personal data do we process?**

We process the data you provide to us in your CV.

On what basis and for what purposes do we process your data?

Your data is processed:

- in order to include your candidacy in future recruitments – based on your consent expressed by sending your CV. You have the right to withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness.

Who do we share your data with – data recipients?

We share your data with:



- entities belonging to the SpeedUp Group, based on the Agreement on the joint control of data – the current list of entities belonging to the SpeedUp Group is available on request.
- subcontractors, i.e. entities we use during the processing of data, with which we have concluded a contract for entrusting the processing of personal data, including: our hosting service provider, our CRM software provider, entities providing IT support services to us, including: provider of the Google Workspace software pack for companies, including e-mail, i.e. Google LLC, whose registered office is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA;
- offices, state authorities and administrative bodies to the extent required by law.

A detailed list of data recipients is available upon your request.

Do we transfer your data outside the European Economic Area, and on what basis?

Be advised that we transfer your data outside the European Economic Area, but these solutions guarantee the legally required level of data security:

- in connection with the use of cookies on our website – read more in the Cookies Policy;
- in connection with the use of the software pack of Google services for companies, including e-mail, where the registered office of Google LLC is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

Thus, your data may be transferred to the United States of America (USA) or other countries outside the European Union, where these companies' servers are located, to the extent of their storage on these servers. In this case, the recipient of your data in the aforementioned third country will be Google LLC

We provide adequate security for your personal data using standard data protection clauses approved by the European Commission and under which certain basic guarantees of the security of your data have been established. Well, all Google services have built-in advanced security features that constantly protect your data and allow you to detect and automatically block potential security threats. The data is protected against unauthorized access, modification, disclosure, or destruction. Security measures include, but are not limited to encryption to ensure data privacy while in transit; a range of security features, such as safe browsing, security checking, and two-step verification of data access; controlling the procedures for collecting, storing, and processing information, including physical security measures to prevent unauthorized access to Google systems. Access to personal data is restricted. Only Google reps who need them in order to process them have it. Any person having such access is obliged to maintain strict confidentiality, and in the event of failure to comply with these obligations, may suffer consequences, including termination of cooperation.

You can find out more about the security of your data in connection with our use of Google's business suite of applications here: https://workspace.google.pl/intl/pl/security/?secure-by-design_activeEl=data-centers

At any time, you have the right to obtain a copy of your personal data transferred to a third country, a copy of contractual clauses, a shortened description of security measures, and a copy of any contract regarding the data subcontracting service.

How long do we process your personal data?

- always for the period necessary to fulfil the purposes of processing, but no longer than until the consent is withdrawn or an objection is raised;
- we process the data obtained for the purpose of providing a response for the period necessary to provide the response/clarify the matter or until you withdraw your consent to data processing, or we determine that the data has become obsolete,

How do we profile and target your data?

Currently, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data.



Is the provision of data obligatory or voluntary?

Providing data is completely voluntary. The consequence of not providing data will be that we will not be able to have your CV for future recruitment purposes.

You may withdraw your consent at any time.

NOTE! Withdrawal of consent, however, does not affect the lawfulness of the processing of your personal data done by us, which we have carried out on the basis of consent expressed prior to its withdrawal.

D. you contact us in other matters:

What kind of personal data do we process?

We process the data you provide to us – these are mainly your contact details, such as: e-mail address, telephone and the content of the inquiry.

On what basis and for what purposes do we process your data?

Your data is processed:

- in order to respond to an inquiry sent to us, based on your consent expressed by sending an inquiry and stating your e-mail address in it – You have the right to withdraw your consent at any time. Withdrawal of consent does not affect the lawfulness of the processing we have carried out on the basis of consent expressed prior to its withdrawal;
- if you contact us for the purpose of concluding a contract – We will process your data in order to take steps aimed at its conclusion;
- in order to conclude a contract for the provision of services toward you as part of our business – based on your interest in our services and actions you undertake with the aim to conclude the contract;
- for evidence purposes, to secure information in the event of a legal need to prove facts and to establish, exercise or defend against legal claims – based on our legitimate interest – balancing test available upon your request. You have the right to object to such processing of your data.

Who do we share your data with – data recipients?

We share your data with:

- entities belonging to the SpeedUp Group, based on the Agreement on the joint control of data – the current list of entities belonging to the SpeedUp Group is available on request.
- subcontractors, i.e. entities we use during the processing of data, with which we have concluded a contract for entrusting the processing of personal data, including: our hosting service provider, our CRM software provider, entities providing IT support services to us, including:
 - ☒ provider of the Google Workspace software pack for companies, including e-mail, i.e. Google LLC, whose registered office is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA;
 - ☒ provider of project management software called "ASANA", i.e. Asana Inc., whose registered office is located at 1550 Bryant Street, Suite 200, San Francisco, CA 94103.
- offices, state authorities and administrative bodies to the extent required by law.

A detailed list of data recipients is available upon your request.

Do we transfer your data outside the European Economic Area, and on what basis?

Be advised that we transfer your data outside the European Economic Area, but these solutions guarantee the legally required level of data security:

- in connection with the use of cookies on our website – read more in the [Cookies Policy](#);



- in connection with the use of the software pack of Google services for companies, including e-mail, where the registered office of Google LLC is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.
- in connection with the use of project management software called "ASANA" provided by Asana Inc., whose registered office is located at 1550 Bryant Street, Suite 200, San Francisco, CA 94103.

Thus, your data may be transferred to the United States of America (USA) or other countries outside the European Union, where these companies' servers are located, to the extent of their storage on these servers. In this case, the recipient of your data in the aforementioned third country will be Google LLC or Asana Inc., respectively, to whom we entrusted the processing of your personal data as a processor.

We provide adequate security for your personal data using standard data protection clauses approved by the European Commission and under which certain basic guarantees of the security of your data have been established. Well, all Google and Asana services have built-in advanced security features that constantly protect your data and allow you to detect and automatically block potential security threats. The data is protected against unauthorized access, modification, disclosure, or destruction. Security measures include, but are not limited to encryption to ensure data privacy while in transit; a range of security features, such as safe browsing, security checking, and two-step verification of data access; controlling the procedures for collecting, storing, and processing information, including physical security measures to prevent unauthorized access to Google or Asana systems. Access to personal data is restricted. Only Google or Asana reps who need them in order to process them have it. Any person having such access is obliged to maintain strict confidentiality, and in the event of failure to comply with these obligations, may suffer consequences, including termination of cooperation.

You can find out more about the security of your data in connection with our use of Google's business suite of applications here:

https://workspace.google.pl/intl/pl/security/?secure-by-design_activeEl=data-centers

You can find more about the security of your data in connection with our use of ASANA software here:

<https://asana.com/security-statement>

At any time, you have the right to obtain a copy of your personal data transferred to a third country, a copy of contractual clauses, a shortened description of security measures, and a copy of any contract regarding the data subcontracting service.

How long do we process your personal data?

- always for the period necessary to fulfil the purposes of processing, but no longer than until the consent is withdrawn or an objection is raised;
- we process the data obtained for the purpose of providing a response for the period necessary to provide the response/clarify the matter or until you withdraw your consent to data processing, or we determine that the data has become obsolete,

How do we profile and target your data?

Currently, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data.

Is the provision of data obligatory or voluntary?

To the extent that data is processed in order to contact you or respond to questions – providing data is voluntary. The consequence of not providing data will be the inability to make contact/ respond.

The consent to the processing of personal data is voluntary. If you do not give us the consent that we ask for, then we will not take the actions to which that consent applies. You may withdraw your consent at any time.

NOTE! Withdrawal of consent, however, does not affect the lawfulness of the processing of your personal data done by us, which we have carried out on the basis of consent expressed prior to its withdrawal.



E. you subscribe to our newsletter:

Remember that we do not jointly control the data of persons subscribing to the newsletter. The controller of your data related to the subscription to the newsletter is: Speedup Management sp. z o.o. with its registered office in Poznań (61-803 Poznań) at ul. św. Marcin 11/8, entered into the Register of Entrepreneurs of the National Court Register under the number KRS 0000265669, NIP 7781440558, REGON 30043371200000, e-mail: gdpr@speedupgroup.com

In order to protect personal data, we have appointed a Data Protection Officer at Ms Monika Synoradzka, who is contacted by e-mail at GDPR@speedupgroup.com or by phone at +48 61 671 01 71, or by correspondence: ul. SW. Marcin 11/8, 61-803 Poznań, Poland.

What kind of personal data is processed?

The form allows you to enter your e-mail address, first and last name. You only need to provide your e-mail address to subscribe. Failure to provide the address will prevent the subscription. Failure to provide the first or last name does not affect the effectiveness of the subscription.

On what basis and for what purposes is your data processed?

Your data is processed for the purpose of sending commercial and marketing information regarding SpeedUp Venture Capital Group and companies included in the SpeedUp Venture Capital Group, in the form of a Newsletter, to the indicated e-mail address – based on your consent.

With whom is your data shared – data recipients?

We share your data with:

- a) subcontractors, i.e. entities we use during the processing of data, with which we have concluded a contract for entrusting the processing of personal data: our hosting service providers, entities providing IT support services to us;
- b) provider of the G-Suit software pack for companies, including e-mail, i.e. Google LLC, whose registered office is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA;
- c) provider of software for managing the newsletter database, i.e. The Rocket Science Group LLC, whose registered office is located at 675 Ponce de Leon Ave NE Suite 5000. Atlanta, GA 30308 USA;
- d) offices, state authorities and administrative bodies to the extent required by law.

A detailed list of data recipients is available upon your request.

Do we transfer your data outside the European Economic Area, and on what basis?

Be advised that we transfer your data outside the European Economic Area, but these solutions guarantee the legally required level of data security:

- in connection with the use of cookies on our website – read more in the [Cookies Policy](#);
- in connection with the use of the software pack of Google services for companies, including e-mail, where the registered office of Google LLC is located at 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.
- in connection with the use of newsletter management software provided by The Rocket Science Group LLC, whose registered office is located at 675 Ponce de Leon Ave NE Suite 5000. Atlanta, GA 30308 USA

Thus, your data may be transferred to the United States of America (USA) or other countries outside the European Union, where these companies' servers are located, to the extent of their storage on these servers. In this case, the recipient of your data in the aforementioned third country will be Google LLC or The Rocket Science Group LLC, respectively, to whom we entrusted the processing of your personal data as a processor.



We provide adequate security for your personal data using standard data protection clauses approved by the European Commission and under which certain basic guarantees of the security of your data have been established. Well, all Google and Asana services have built-in advanced security features that constantly protect your data and allow you to detect and automatically block potential security threats. The data is protected against unauthorized access, modification, disclosure, or destruction. Security measures include, but are not limited to encryption to ensure data privacy while in transit; a range of security features, such as safe browsing, security checking, and two-step verification of data access; controlling the procedures for collecting, storing, and processing information, including physical security measures to prevent unauthorized access to Google or Asana systems. Access to personal data is restricted. Only Google or The Rocket Science Group reps who need them in order to process them have it. Any person having such access is obliged to maintain strict confidentiality, and in the event of failure to comply with these obligations, may suffer consequences, including termination of cooperation.

You can find out more about the security of your data in connection with our use of Google's business suite of applications here:

https://workspace.google.pl/intl/pl/security/?secure-by-design_activeEI=data-centers

You can find more about the security of your data in connection with our use of The Rocket Science Group software here: <https://mailchimp.com/about/security/>

At any time, you have the right to obtain a copy of your personal data transferred to a third country, a copy of contractual clauses, a shortened description of security measures, and a copy of any contract regarding the data subcontracting service.

How long do we process your personal data?

Your data will be processed for the period necessary to fulfil the indicated purposes of processing, but no longer than UNTIL THE CONSENT IS WITHDRAWN OR AN OBJECTION IS RAISED, or the Newsletter is no longer issued.

How do we profile and target your data?

Currently, we do not use automated processing, consisting in making decisions in individual cases, including profiling, in relation to your data. However, be advised that the technique used for sending the newsletters enables us to determine if and when the e-mail was opened by the subscriber as well as which of the links contained in the e-mail were activated by them. Such information is stored by the newsletter system and analysed by us in order to optimise the delivery of the newsletter and to better adapt the content of future newsletters to the interests of subscribers.

Is the provision of data obligatory or voluntary?

Providing personal data is voluntary, however, without an e-mail address, it will be impossible for us to provide the Newsletter.

The consent to the processing of personal data is voluntary. If you do not give us the consent that we ask for, then we will not take the actions to which that consent applies. You may withdraw your consent at any time.

NOTE! Withdrawal of consent, however, does not affect the lawfulness of the processing of your personal data done by us, which we have carried out on the basis of consent expressed prior to its withdrawal.

[E. you use our website www.hugething.vc:](http://www.hugething.vc)

What kind of personal data do we process?

We process data collected by cookies located on our Website. As a rule, cookies do not constitute personal data. However, certain information stored in cookies (e.g. in regard to preferences), especially when combined with other information about the website user, may be considered personal data. Personal data collected by using cookies may be processed only in order to perform certain functions for the user, described above. Such data is encrypted in a manner which prevents unauthorised persons from accessing it. More in our [Cookies policy](#).



On what basis and for what purposes do we process your data?

If you browse our Websites – the processing of personal data from cookies is carried out:

- for analytical and statistical purposes – on the basis of our legitimate interest consisting in conducting analyses of Users' activity, as well as their preferences in order to improve the functionalities used and services provided – balancing test available upon your request. You have the right to object to such processing of your data.

More in [Cookies policy](#).

The Users' activity on the Website, including their personal data, is recorded in system logs (a special computer program used for storing a chronological record containing information on the use of the Website). We also process the information collected in the logs for technical purposes, in particular the data may be temporarily stored and processed in order to ensure the security and proper functioning of IT systems, e.g. in connection with creating backups, testing changes in IT systems, detecting irregularities or protecting against misuse and attacks.

Who do we share your data with data recipients?

We share your data with:

- entities belonging to the SpeedUp Group, based on the Agreement on the joint control of data – the current list of entities belonging to the SpeedUp Group is available on request.
- when the Website is loaded – cookies from external providers are installed on your end device, which collect data about you and disclose it to these providers – more on this subject in [Cookies policy](#).
- offices, state authorities and administrative bodies to the extent required by law.

A detailed list of data recipients is available upon your request.

Do we transfer your data outside the European Economic Area, and on what basis?

Be advised that we transfer your data outside the European Economic Area, but these solutions guarantee the legally required level of data security:

- in connection with the use of cookies on our website – more in [Cookies policy](#);

How long do we process your personal data?

- always for the period necessary to fulfil the purposes of processing, but no longer than until the consent is withdrawn or an objection is made;
- in the case of data collected by cookies – depending on a given cookie – more in [Cookies policy](#).

How do we profile and target your data?

We do not use targeted advertising or profiled advertising on our Website.

Is the provision of data obligatory or voluntary?

In the case of our Website being loaded for viewing, we collect only the data that is necessary to display it – without downloading it, it would be impossible to display the page – as well as data the downloading of which is based on our legitimate interest (unless you have excluded this possibility by appropriately configuring your browser). More in [Cookies policy](#).

You have the right to object to such processing of your data.

G. you click on social media plugins located on our Website or use our social media accounts:

Our Website uses the so-called social plugins for social media such as: Facebook, Twitter, LinkedIn, Crunchbase, Angel.co. After the user enters the website, the data is not automatically sent to the above-mentioned social networks. Data will only be sent to these social networks if the user actively clicks on the corresponding button of a social network. In this case, the browser will start connecting to the servers of the given social network. By clicking on the appropriate button (e.g. the ICON of a given social network), the



user agrees that their browser will generate a link to the servers of the given social network and transfer data about the user to the respective operator of the social network and vice versa. We have no influence on the nature and scope of the data collected by the social networks.

The social network provider stores the collected user data as a user profile and uses it for the purposes of advertising, market research and/or the design of an audience-oriented website. Such assessment takes place in particular (also for users who are not logged in) to provide fair advertising for the audience and to inform other users of the social network about the user's activities on our website. The user has the right to object to the creation of user profiles, although the provider of the relevant plugin must be contacted in order to exercise this right. Thanks to the plugins, we offer the possibility to interact with social networks and other users, so that we can improve our offer and make it more interesting.

The data is transferred regardless of whether the user has an account with the plugin provider and is logged in there. If the user is logged in with the respective plugin provider, the collected data will be directly assigned to the existing user account. After clicking the activated button and (for example) linking the page, the plugin provider stores this information in user's account and makes it publicly available to the user's friends. We recommend logging out regularly after using a social network, especially before activating the button, as this way one can avoid assigning their profile by the plugin provider.

We have included icons for the following social media on the website:

- Facebook – the provider is Facebook Inc.
- twitter – the provider is Twitter Inc.
- LinkedIn – the provider is LinkedIn Inc.
- Crunchbase – the provider is Crunchbase Inc. based in San Francisco, USA.
- Angel.co – the provider is AngelList Holdings, LLC based in San Francisco, USA.

These providers process your data for their own purposes that are not known to us – as a data controller separate from us. Processing causes the transfer of your personal data outside the European Economic Area. At the same time, these providers are certified within the scope of the Privacy Shield agreement between the EU and the USA, which ensures an adequate level of data protection required in the European Union.

For more information on the purpose and scope of the data collection and its processing by the plugin provider, please refer to the providers' data protection declarations shown below. The following providers will further inform the user on their rights in this regard and will establish an option in the settings to protect their privacy.

- Facebook – https://www.facebook.com/legal/FB_Work_Privacy,
- Twitter – <https://twitter.com/en/privacy>,
- LinkedIn – <https://www.linkedin.com/legal/privacy-policy>,
- Crunchbase – <https://about.crunchbase.com/terms-of-service/gdpr-privacy-policy>
- Angel.co – <https://angel.co/privacy>.

At the same time, we are the Controller of your data, which we collect in connection with your use of our profiles and accounts on social networks. More about this processing in individual GDPR informational clauses for individual accounts: [Facebook](#), [Twitter](#), [LinkedIn](#). The rules of the processing of your personal data, its sharing and processing time depend on the account you use. In case of using our social media accounts, providing data is voluntary, but the consequence of not providing data will be the inability to browse the fanpage or leave comments.

§6 Changes to the Privacy Policy.

We reserve the right to make changes to this Policy, which may result from the need to adapt to changes in law or applicable privacy standards, or expanding our offer. In connection with the above, we will inform you about any significant changes to this Policy via an appropriate message on our websites. The message will be presented in a visible way, it will inform about the content of the introduced changes and their consequences for your data. Each time, the date of introducing changes will be determined so that the message about them appears in sufficient time to get acquainted with the content of the message, consider the nature and impact of the changes on the processing of your data. The date will take into account the necessity to create



appropriate time frame for you to exercise your rights under the GDPR (e.g. withdrawal of consent or objection to processing).

