DANISH BUSINESS AUTHORITY

Data Processing Agreement

between

the Data Controller:

the Danish Business Authority

Business Reg. no. 10150817

Langelinie Allé 17

2100 Copenhagen Ø

Denmark

and

the Data Processor

[Name]

Business Reg. no. [Business Reg. no.]

[Address]

[Postcode and town]

[Country]

1 Contents

2 Background to the Data Processing Agreement

1. This Agreement determines the rights and obligations that apply when the Data Processor processes personal data on behalf of the Data Controller.

2. The agreement is designed to facilitate the parties' compliance with Article 28 (3) *of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural person with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)* which sets specific requirements for the content of a Data Processing Agreement.

3. The Data Processor processes personal data in order to fulfil the parties' "Main Agreement": Service of the Startup Denmark Secretariat and expert panel 2019-2021, entered into on [date].

4. The Data Processing Agreement and the "Main Agreement" are interdependent and cannot be terminated separately. However, the Data Processing Agreement can – without terminating the "Main Agreement" – be replaced by another valid Data Processing Agreement.

5. This Data Processing Agreement takes precedence over any corresponding provisions in other agreements between the parties, including those in the "Main Agreement".

6. This agreement has 4 appendices. The appendices are an integral part of the Data Processing Agreement.

7. The Data Processing Agreement Bilag A contains details of the processing, including the purpose and nature of the processing, the type of personal data, the categories of recorded data and the duration of the processing.

8. The Data Processing Agreement Bilag B contains the Data Controller's conditions for the Data Processor's use of any sub-processors, as well as a list of any sub-processors approved by the Data Controller.

9. The Data Processing Agreement Bilag C contains detailed instructions on the type of processing that the Data Processor carries out on behalf of the Data Controller (the subject of the processing), the minimum security measures to be implemented and the supervision of the Data Processor and any sub-processors.

10. The Data Processing Agreement and appendices shall be stored in writing, including electronically, by both parties.

11. This Data Processing Agreement does not release the Data Processor from obligations directly imposed on the Data Processor in accordance with the General Data Protection Regulation or any other law.

3 The Data Controller's obligations and rights

1. The Data Controller is responsible to the outside world (including the data subject), for ensuring that the personal data is processed within the framework of the General Data Protection Regulation and the Data Protection Act.

2. The Data Controller has, therefore, both the right and the obligation to make decisions on the purpose of the processing and on which aids must be used.

3. The Data Controller is, among other things, responsible for ensuring that there is a legal basis for the processing that the Data Processor is instructed to carry out.

4 The Data Processor acts according to instructions

1. The Data Processor may only process personal data according to the documented instructions from the Data Controller, unless required by EU law or the national laws of the Member State to which the Data Processor is subject; in which case, the Data Processor must inform the Data Controller of this legal requirement prior to processing, unless the relevant court prohibits such disclosure due to important societal interests cf. Article 28 (3) (a).

2. The Data Processor shall immediately inform the Data Controller if a Data Processor's instruction is in violation of the General Data Protection Regulation or data protection provisions in other EU law or the national law of Member States.

5 Confidentiality

1. The Data Processor ensures that only those persons currently authorised to do so have access to the personal data processed on behalf of the Data Controller. Access to the information must therefore be terminated immediately if the authorisation is withdrawn or expires.

2. Individuals may only be authorised if they need access to the personal data in order to fulfil the Data Processor's obligations to the Data Controller.

3. The Data Processor shall ensure that the persons authorised to process personal data on behalf of the Data Controller are committed to confidentiality or are subject to appropriate statutory duty of confidentiality.

4. At the request of the Data Controller, the Data Processor must be able to demonstrate that the relevant employees are subject to the abovementioned confidentiality obligation.

6 Processing security

1. The Data Processor implements all the measures required under Article 32 of the General Data Protection Regulation, which states that, inter alia, while taking into account the current level, the cost of implementation and the nature, scope, coherence and purpose of the relevant processing, and the risks of varying probability and severity to the rights and freedoms of natural persons, appropriate technical and organisational measures must be implemented to ensure a level of security which is appropriate for these risks.

2. The above obligation implies that the Data Processor must carry out a risk assessment and then implement measures to address identified risks. This may include, inter alia, as appropriate, the following measures:

    a. Pseudonymisation and encryption of personal data
    b. Capacity to ensure continuous confidentiality, integrity, accessibility and robustness of processing systems and services
    c. Capacity to restore, in a timely manner, the availability of and access to personal data in the event of a physical or technical incident
    d. The Data Processor must have a procedure for the regular testing, assessment and evaluation of the effectiveness of technical and organisational measures in ensuring the security of the processing.

3. The Data Processor must, in connection with the above – in all cases – at least implement the level of security and the measures specified in Appendix C to this Agreement.

4. The parties' possible regulation/agreement on remuneration or similar, in connection with the Data Controller or Data Processor's subsequent requirements for the establishment of additional security measures, will be stated in the parties' "Main Agreement" and Appendix D of this Agreement.

7 Use of sub-processors

1. The Data Processor must comply with the conditions specified in Article 28 (2) and (4) of the General Data Protection Regulation on using another Data Processor (sub-processor).

2. Thus, the Data Processor may not use another Data Processor (sub-processor) to fulfil the Data Processing Agreement without the prior specific or general written approval of the Data Controller.

3. In the case of general written approval, the Data Processor must notify the Data Controller of any planned changes regarding the addition or replacement of other Data Processors, thereby allowing the Data Controller to object to such changes.

4. The Data Controller's terms and conditions for the Data Processor's use of any sub-processors are specified in Bilag B of this Agreement.

5. The Data Controller's approval of specific sub-processors, if any, is stated in Bilag B of this Agreement.

6. When the Data Processor has the Data Controller's consent to use a sub-processor, the Data Processor undertakes to impose the same data protection obligations as those specified in this Data Processing Agreement through a sub-processor agreement or other legal document pursuant to EU law or the national law of Member States, specifically providing the necessary guarantees that the sub-processor will implement the appropriate technical and organisational measures in such a way that the processing complies with the requirements of the General Data Protection Regulation.

   By entering into a sub-processing agreement, the Data Processor is thus responsible for, at minimum, imposing on any sub-data processor the obligations that the Data Processor itself is subject to according to the data protection rules and this Data Processing Agreement and appendices.

7. The sub-processing agreement and any subsequent changes thereto are sent, at the request of the Data Controller, as a copy to the Data Controller, who thereby has the opportunity to make sure that a valid agreement has been entered into between the Data Processor and the sub-processor. Any commercial terms, such as prices, that do not affect the legal data protection content of the sub-processor agreement, must not be sent to the Data Controller.

8. The Data Processor, in its agreement with the sub-processor, must include the Data Controller as a beneficiary third party in the case of the Data Processor's bankruptcy, so that the Data Controller can enter the Data Processor's rights and apply them to the sub-processor, so that, for example, the Data Controller can instruct the sub-processor to delete or return information.

9. If the sub-processor does not fulfil its data protection obligations, the processor remains fully liable to the Data Controller for the fulfilment of the sub-processor's obligations.

8 Transfer of data to recipients in third countries, including international organisations

1. The Data Processor may only process personal data following documented instructions from the Data Controller, including with regard to transfer (making available, forwarding and internal use) of personal data to third countries or international organisations, unless required under EU law or the national law of the Member State to which the Data Processor is subject; in which case, the Data Processor must inform the Data Controller of this legal

requirement before the processing takes place, unless the applicable law prohibits such notification for reasons of important societal interests, see Article 28 (3) (a).

2. Without the Data Controller's instructions or approval, the Data Processor cannot – within the framework of the Data Processing Agreement – inter alia:

    a. transfer personal data to a Data Controller in a third country or international organization,
    b. transfer the processing of personal data to a subcontracting Data Processor in a third country, or
    c. allow the data to be processed in a different department of the Data Processor that is located in a third country.

3. The Data Controller's instructions or approval for the transfer of personal data to a third country will be stated in Bilag C of this Agreement.

9 Assistance for the Data Controller

1. Taking into account the nature of the processing, the Data Processor shall assist, as much as possible, the Data Controller with appropriate technical and organisational measures, to fulfil the Data Controller's obligation to respond to requests for exercising the rights of data subjects as stipulated in chapter III of the General Data Protection Regulation.

    This means that the Data Processor must, as much as possible, assist the Data Controller in its obligation to ensure compliance with:

    a. the obligation to provide information when collecting personal data from the data subject
    b. the obligation to provide information if personal data is not collected from the data subject
    c. the data subject's right of access
    d. right to rectification
    e. the right of deletion (the right to be forgotten)
    f. the right to restrict processing
    g. duty of notification in connection with the rectification or deletion of personal data or restriction on processing
    h. the right to data portability
    i. the right to object
    j. the right to object to the outcome of automatic individual decisions, including profiling

2. The Data Processor assists the Data Controller in ensuring compliance with the Data Controller's obligations under Articles 32-36 of the General Data Protection Regulation, taking

into account the nature of the processing and the information available to the Data Processor in accordance with Article 28 (3) (f).

This means that the Data Processor, taking into account the nature of the processing, must assist the Data Controller in its obligation to ensure compliance with:

a. the obligation to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks associated with the processing.
b. the obligation to notify personal data breaches to the supervisory authority (the Danish Data Protection Agency) without undue delay and, if possible, within 72 hours of the Data Controller becoming aware of the breach, unless it is unlikely that the breach of personal data security poses a risk to the rights or freedoms of natural persons.
c. the obligation to notify the data subject(s), without undue delay, of a breach of personal data security when such breach is likely to pose a high risk to the rights and freedoms of natural persons.
d. the obligation to carry out a data protection impact assessment if a type of processing is likely to pose a high risk to the rights and freedoms of natural persons.
e. the obligation to consult the supervisory authority (the Danish Data Protection Agency) before processing, if a data protection impact assessment shows that the processing will lead to high risk in the absence of measures implemented by the Data Controller to mitigate the risk

3. The parties' regulation/agreement on remuneration for the Data Processor's assistance to the Data Controller will be stated in the parties' "Main Agreement" and Appendix D of this Agreement.

10 Notification of breaches of personal data security

1. The Data Processor must inform the Data Controller without undue delay after becoming aware that there has been a breach of personal data security with the Data Processor or any sub-processor.

   The Data Processor must notify the Data Controller as soon as possible and no later than 24 hours after it has become aware of the breach, so that the Data Controller has the opportunity to comply with any obligation to report the breach to the supervisory authority within 72 hours.

2. In accordance with paragraph 10.2 (b) of this Agreement, the data processor must – taking into account the nature of the processing and the information available to it – assist the Data Controller in notifying the breach to the supervisory authority.

This may mean that the Data Processor must help provide the following information which, according to Article 33 (3) of the General Data Protection Regulation, must be stated in the Data Controller's notification to the supervisory authority:

a. The nature of the breach of personal data security, including, where possible, the categories and approximate number of data subjects concerned as well as the categories and the approximate number of personal data records concerned
b. Likely consequences of the breach of personal data security
c. Measures implemented or proposed to be implemented to address the breach of personal data security, including, where appropriate, measures to limit its possible negative effects

11 Deletion and return of information

1. Upon termination of the processing services, the Data Processor is obliged, at the discretion of the Data Controller, to delete or return all personal data to the Data Controller, and to delete existing copies, unless EU law or national law requires the retention of personal data.

12 Supervision and auditing

1. The Data Processor makes available all the information necessary to demonstrate the Data Processor's compliance with Article 28 of the General Data Protection Regulation and with this Agreement to the Data Controller, and allows and contributes to audits, including inspections, carried out by the Data Controller or another auditor authorised by the Data Controller.

2. The detailed procedure for the Data Controller's supervision of the Data Processor is stated in Bilag C of this Agreement.

3. The Data Controller's supervision of any sub-processors generally takes place through the Data Processor. The detailed procedure for this is stated in this Agreement's Bilag C.

4. The Data Processor is obliged to provide access to its physical facilities to the authorities which, according to the law in force at any given time, have the right to access the Data Controller's and Data Processor's facilities or to representatives acting on the behalf of such authorities, against suitable identification.

13 Entry into force and termination

1. This Agreement will enter into force upon signature by both parties.

2. Either party may demand that the Agreement be renegotiated in the event of changes in law or inappropriate matters in the Agreement.

3. The parties' possible regulation/agreement on remuneration, conditions etc. in connection with changes to this Agreement will be stated in the parties' "Main Agreement" or Appendix D of this Agreement.

4. The Data Processing Agreement may be terminated in accordance with the terms of termination, including notice of termination as stated in the "Main Agreement".

5. The Agreement is valid for as long as the processing continues. Regardless of the termination of the "Main Agreement" and/or the Data Processing Agreement, the Data Processing Agreement will remain in effect until the processing ceases and the deletion of the data by the Data Processor and any sub-processors.

6. Signature

On behalf of the Data Controller

Name: [Enter name]

Position: [Enter position]

Date: [Enter date]

Signature: [Provide signature]

On behalf of the Data Processor

Name: [Enter name]

Position: [Enter position]

Date: [Enter date]

Signature: [Provide signature]

14 Contact persons/contact points with the Data Controller and the Data Processor

1. The parties can contact each other via the contact persons/contact points below:

2. The parties are obliged to regularly inform each other about changes regarding the contact person/contact point.

Name: [Enter name]

Position: [Enter position]

Telephone number: [Enter telephone number]

Email address: [Enter email address]

Name: [Enter name]

Position:	[Enter position]	Email address:	[Enter email address]
Telephone number:	[Enter telephone number]		

Bilag A Information on processing

The purpose of the Data Processor's processing of personal data on behalf of the Data Controller is that the Data Controller can use the system, which is owned and managed by the Data Processor, to collect and process information about Startup Denmark applicants, applications and evaluations from the Startup Denmark expert panel.

The Data Processor's processing of personal data on behalf of the Data Controller primarily concerns that the Data Processor makes data from the system available to the Data Controller through a system integration (application programming interface) and thereby stores personal data about Startup Denmark applicants and the Startup Denmark expert panel on the company's servers.

The processing includes the following types of personal information about the data subjects: Name, email address, address, nationality, birthday, sex, area of responsibility in the company, educational level, data of completion of education, result of evaluation, application date, and application-id.

The processing includes the following categories of data subjects: People who applies with a personal business idea in Startup Denmark.

The Data Processor can begin to process personal data on behalf of the Data Controller after the entry into force of this Agreement. The processing has the following duration: The processing is time-limited and shall last until the Agreement ends or is terminated by one of the parties.

Bilag B Conditions for the Data Processor's use of sub-processors and list of approved sub-processors

B.1 Conditions for the Data Processor's use of any sub-processors

A sub-processor is any natural or legal person, a public authority, institution or other body that assists the Data Processor in the processing of personal data on behalf of the Data Controller.

The Data Processor must only use sub-processors with the prior specific written approval of the Data Controller. The Data Processor's request for this must be submitted to the Data Controller at least 2 months before the application or the change shall take effect. The Data Controller can only refuse approval if the Data Controller has reasonable, specific reasons to do so.

B.2 Approved sub-processors

Upon entry into force of the Data Processing Agreement, the Data Controller has approved the use of the following sub-processors:

Name	Business Reg. no.	Address	Description of processing
[Name]	[Business Reg. no.]	[Address]	[General description of the processing by the sub-processor]
[Name]	[Business Reg. no.]	[Address]	[General description of the processing by the sub-processor]
[Name]	[Business Reg. no.]	[Address]	[General description of the processing by the sub-processor]
[Name]	[Business Reg. no.]	[Address]	[General description of the processing by the sub-processor]

Upon entry into force of the Data Processing Agreement, the Data Controller has specifically approved the use of the above-mentioned sub-processors for the specific processing described above for the party. The Data Processor cannot, without the Data Controller's specific and written approval, use the individual sub-processor for a "different" processing than what was agreed, nor let another sub-processor undertake the described processing.

Bilag C Instructions for processing personal data

C.1 The subject of the processing/instructions

The Data Processor processes the personal data on behalf of the Data Controller by carrying out the following:

- Receiving applications from individuals to Startup Denmark and related evaluations from the Startup Denmark expert panel, cf. "Main Agreement".
- At the Data Controller's request, the Data Processor must be able to provide information about tasks in which personal data has been accessed.
- Data, including extractions of production data, must be stored both physically and technically in such a way that unauthorised persons cannot access the personal data contained therein.
- The Data Processor must not remove data from the Data Controller's production environment, unless there is a written approval from the Data Controller.

C.2 Processing security

The Data Processor will initiate the level of security and all measures required in accordance with the Data Processing Agreement and the instructions of the Data Controller, cf. Appendix C.1, any data security requirements that are specified in the Main Agreement and its appendices, and otherwise in accordance with the General Data Protection Regulation, Article 32.

Given this, and taking into account the current technical level, implementation costs and the nature, scope, context and purpose of the processing, as well as the risks of varying probability and severity to the rights and freedoms of natural persons, the Data Processor will conduct the appropriate technical and organisational measures to ensure a level of security that is appropriate for these risks.

What constitutes appropriate technical and organisational measures must also be assessed in relation to the specific system, the purpose of the processing and the type of personal data.

In the assessment of the appropriate level of security, consideration will also be given to the risks posed by the processing, namely in the event of accidental or illegal destruction, loss, alteration, unauthorised disclosure or access to personal data that has been transmitted, stored or otherwise processed.

The above obligation implies that the Data Processor must conduct a risk assessment for the data subjects that are linked to the ongoing risk assessment of the Data Processor in accordance with ISO 27001 and then implement measures to address identified risks. Depending on what is relevant and thus established in the instructions and any data security requirements as specified in the Main Agreement and its appendices, this may include the following measures:

<u>Encryption of personal data</u>

The Data Processor shall develop guidelines for securing external communication lines and must take measures to ensure that those who are unauthorised cannot access data through these connections.

Anonymisation/pseudonymisation of test data
The Data Controller is responsible for designing the test data, including anonymisation or pseudonymisation of this data. The Data Processor implements the test data provided by the Data Controller in the relevant systems and solutions.

Accessibility
The Data Processor must be able to restore the availability and access to personal data in a timely manner in the event of an accidental physical or technical incident.

Logging
The Data Processor must ensure that event logging for recording user activity, exceptions, errors and information security events is stored and reviewed. The Data Processor must protect logging facilities and log data from manipulation and unauthorised access.

The Data Processor must ensure that automated registration (logging) of all uses of personal data is carried out. At a minimum, the registration must contain information about the time, user, type of use and indication of the person to whom the used data relates or the search criteria used. The log must be kept for 6 months, after which it will be deleted.

The Data Processor must ensure that activities conducted by the system administrators and system operators are logged, and the Data Processor must use these logs and review them regularly. The logs must be kept for 6 months, after which they will be deleted.

Processing security and risk assessment
The Data Processor must ensure continued confidentiality, integrity, accessibility and robustness of processing systems and services.

If the Data Processor becomes aware, including as part of its ongoing risk assessment, that the actions required by the Data Controller are not sufficient or appropriate, the Data Processor must, immediately after being made aware, inform the Data Controller in writing and assist the Data Controller in taking appropriate technical and organisational measures. The Data Processor is therefore obliged to continuously assess whether the security level is appropriate and, if necessary, to adjust the processing accordingly. Assistance in relation to this is settled according to time spent, cf. Appendix D, provided that a written agreement has been reached on the content and scope of the specific assistance.

The Data Processor must have a procedure for regular testing, assessment and evaluation of the effectiveness of technical and organisational measures in ensuring the security of the processing.

Upon request by the Data Controller, the Data Processor must provide the Data Controller with sufficient information to enable the Data Controller to document that the Data Processor has taken the necessary technical and organisational security measures, cf. Appendix C.6 regarding supervision.

C.3 Retention period/Deletion procedure

The personal information shall be stored for the duration of the contract and must then be deleted from the Data Processor. The Data Processor must comply, if the Data Controller requests the immediate deletion of all personal information or parts thereof.

In cases in which personal data is processed at multiple physical locations and personal data may be stored in several locations, the Data Controller must ensure that all personal data is deleted from all storage media that have been used. The Data Controller must ensure that all copies of the personal data can and will be identified and ultimately deleted.

C.4 Processing location

The personal data covered by the agreement may not be processed at locations other than the following, without the Data Controller's prior written approval:

- [Specify where the processing takes place] [Specify which data processor or sub-processor uses the address]

C.5 Instructions or approval for the transfer of personal data to third countries

The Data Processor may only conduct transfer (making available, forwarding and internal use) of personal data to third countries or international organisations following documented instruction or approval from the Data Controller, unless required under EU law or the national law of the Member State to which the Data processor is subject; in which case, the Data Processor must inform the Data Controller of this legal requirement before the processing takes place, unless the applicable law prohibits such notification for reasons of important societal interests, cf. Article 28 (3) (a).

Thus, the Data Processor may not make independent decisions regarding, inter alia:

a. forwarding personal data to a Data Controller in a third country,
b. transferring the processing of personal data to a sub-processor in a third country, or
c. allowing the data to be processed in a different department of the Data Processor that is located in a third country.

The Data Controller can only approve a transfer of personal data to a third country when there is an authorisation for forwarding the personal data in addition to a basis for transfer in accordance with Chapter V of the General Data Protection Regulation. A basis for transfer may, for example, be safeguards required under the standard provisions of the Commission, cf. Article 46 (2) (c), or because the third country concerned has been approved by the Commission as a safe third country, cf. Article 45. It is indicated in the General Data Protection Regulation Article 46 (2) (f) that the guarantees required with respect to a transfer to an insecure third country can be secured through an approved certification mechanism together with binding and enforceable commitments of the Data Controller or Data Processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights

C.6 Detailed procedures for the Data Controller's supervision of the processing carried out by the Data Processor

On an annual basis and at its own expense, the Data Processor must obtain an audit statement from an independent third party regarding the compliance of the Data Processor with this Data Processing Agreement and its appendices.

The Parties agree that the following types of audit statement can be used: ISAE 3000 and ISAE 3402.

If other types of audit statement are used, the Data Processor must demonstrate that these have the same minimum level of protection as the statements mentioned above.

The audit statement must be sent to the Data Controller for information purposes as soon as possible after receipt.

The Data Controller or a representative for the Data Controller must also have access to conduct an inspection including a physical inspection, at the Data Processor, when the Data Controller considers this to be necessary.

C.7 Further procedures for the Data Controller's supervision of the processing carried out by the Data Processor

On an annual basis and at its own expense, the Data Processor shall obtain an audit statement from an independent third party regarding the compliance of the Data Processor with this Data Processing Agreement and its appendices.

The Parties agree that the following types of audit statement can be used: ISAE 3000 and ISAE 3402.

If other types of audit statement are used, the Data Processor must demonstrate that these have the same minimum level of protection as the statements mentioned above.

The audit statement must be sent to the Data Controller for information purposes as soon as possible after receipt.

The Data Processor or a representative for the Data Processor must also have access to conduct an inspection, including a physical inspection at the Data Processor, when the Data Processor (or the Data Controller) considers this to be necessary.

The documentation for inspections that have been carried out must be sent to the Data Controller as soon as possible for information purposes.