**DATA PROCESSING AGREEMENT**

Content

[1. PARTIES, POSITION OF THE PARTIES, CONTACT AND CONTACT DETAILS 2](#_Toc183165183)

[2. DEFINITIONS 2](#_Toc183165184)

[3. BACKGROUND AND AIM 3](#_Toc183165185)

[4. PROCESSING OF PERSONAL DATA AND SPECIFICATION 4](#_Toc183165186)

[5. OBLIGATIONS OF THE CONTROLLER 4](#_Toc183165187)

[6. OBLIGATIONS OF THE PROCESSOR 4](#_Toc183165188)

[7. SECURITY MEASURES 5](#_Toc183165189)

[8. SECRECY/DUTY OF CONFIDENTIALITY 5](#_Toc183165190)

[9. INSPECTION, SUPERVISION AND AUDITING 6](#_Toc183165191)

[10. HANDLING OF CORRECTIONS AND DELETIONS ETC 7](#_Toc183165192)

[11. PERSONAL DATA BREACHES 7](#_Toc183165193)

[12. SUB-PROCESSOR 7](#_Toc183165194)

[13. LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY 8](#_Toc183165195)

[14. LIABILITY FOR DAMAGE IN CONNECTION WITH PROCESSING 9](#_Toc183165196)

[15. CONCLUSION, TERM AND TERMINATION OF THIS AGREEMENT 9](#_Toc183165197)

[16. AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECTS, ETC 9](#_Toc183165198)

[17. MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT 10](#_Toc183165199)

[18. NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND INSTRUCTIONS 10](#_Toc183165200)

[19. CONTACT PERSONS 11](#_Toc183165201)

[20. RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS AND CONTACT INFORMATION 11](#_Toc183165202)

[21. CHOICE OF LAW AND DISPUTES 11](#_Toc183165203)

[22. THE PARTIES’ SIGNATURES ON THE AGREEMENT 11](#_Toc183165204)

[Annex 1 – Instructions for the Processing of Personal Data 13](#_Toc183165205)

[Annex 2 – List of approved Sub-processors 16](#_Toc183165206)

DATA PROCESSING AGREEMENT

Agreements pursuant to Article 28(3) of the General Data Protection Regulation EU 2016/679[[1]](#footnote-2)

1. PARTIES, POSITION OF THE PARTIES, CONTACT AND CONTACT DETAILS

|  |  |
| --- | --- |
| Controller | Processor |
| Mid Sweden University  | [Full name of the organization] |
| Organization number | Organization number |
| 202100-4524 | [Organization registration number] |
| Postal address | Postal address |
| 851 70 Sundsvall831 25 Östersund | [Organization’s postal address] |
| Contact person for the administration of this Data Processing Agreement  | Contact person for the administration of this Data Processing Agreement |
| Name: *[Contact person's First name and Last name]*E-mail: *[Contact person's email address]*Tel: *[Contact person's phone number]* | Name: *[Contact person's First name and Last name]*E-mail: *[Contact person's email address]*Tel: *[Contact person's phone number]* |
| Contact person for the Parties' cooperation on data protection  | Contact persons for the parties' cooperation on data protection |
| E-mail: dataskyddsombud@miun.se | E-mail: *[Contact person's email address]* |

2. DEFINITIONS

In addition to the terms defined in the text of this Data Processing Agreement, these definitions, whether used in plural or singular, in definite or indeterminate form, shall have the following meanings when they are indicated in capital letters as the initial letter.

|  |  |
| --- | --- |
| Processing | Any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; |
| Data protection legislation | Refers to all privacy and personal data legislation, along with any other legislation (including regulations and directives) applicable to the Processing carried out in accordance with this Agreement, including national and EU legislation.  |
| Controller | Any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.  |
| Instruction | The written instructions that more specifically define the object, duration and purpose of Personal Data, as well as the categories of Data Subjects and special requirements that apply to the Processing.  |
| Log | A Log is the result of Logging. |
| Logging | Logging is the continuous collection of information about the Processing of Personal Data that is performed according to this Agreement and which can be associated with an individual natural person.  |
| Processor | A natural or legal person, public authority, agency or other body that Processes Personal Data on behalf of the Controller. |
| Personal Data | Any information relating to an identified or identifiable natural person, where an identifiable natural person is a person who directly or indirectly can be identified in particular by reference to an identifier such as name, social security number, location data or online identifiers or one or more factors which are specific to the natural person's physical, physiological, genetic, psychological, economic, cultural or social identity.  |
| Personal Data Breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.  |
| Data Subject  | Natural person whose Personal Data is Processed. |
| Third country | A state that is not a member of the European Union (EU) or the European Economic Area (EEA). |
| Sub-processor | A natural or legal person, public authority, agency or other body that, as a subcontractor to the Processor, Processes Personal Data on behalf of the Controller.  |

3. BACKGROUND AND AIM

3.1 Through this Agreement, the Instructions and a list of possible Sub-processors (hereafter jointly referred to as “the Agreement”), the Controller regulates Processor’s Processing of Personal Data on behalf of the Controller. The aim of the Agreement is to safeguard the freedoms and rights of the Data Subject during Processing, in accordance with what is stipulated in Article 28(3) of the General Data Protection Regulation (EU) 2016/679 (“GDPR”).

3.2 Where this Agreement forms one of several contractual documents within the framework of another agreement, the second agreement is referred to as the ‘Main Agreement’ in this Agreement.

3.3 If anything stipulated in item 1, paragraph 3.2, item 165 or 16, paragraph 18.6, items 19–20 or 23 in this Agreement is otherwise regulated in the Main Agreement, the regulation of the Main Agreement shall have precedence.

3.4 References in this Agreement to national or EU legislation refer to the applicable regulations at any given time.

4. PROCESSING OF PERSONAL DATA AND SPECIFICATION

4.1 The Controller hereby appoints the Processor to carry out the Processing on behalf of the Controller in accordance with this Agreement.

4.2 The Controller shall give written Instructions to the Processor on how to carry out the Processing.

4.3. The Processor may only carry out the Processing in accordance with this Agreement and the Instructions in force at any given time.

5. OBLIGATIONS OF THE CONTROLLER

5.1 The Controller is responsible for ensuring that there is a legal basis for the Processing at all times and for compiling correct Instructions with regard to the nature of the Processing so that the Processor and any Sub-processor can fulfil their tasks according to this Agreement and the Main Agreement, where applicable.

5.2 The Controller shall, without undue delay, inform the Processor of any changes in the Processing that affect the Processor's obligations pursuant to Data Protection Legislation.

5.3 The Controller is responsible for informing the Data Subject about the Processing and for safeguarding the Data Subject's rights under the Data Protection Legislation as well as taking any other action incumbent on the Controller according to Data Protection Legislation.

6. OBLIGATIONS OF THE PROCESSOR

6.1 The Processor undertakes to only carry out the Processing in accordance with this Agreement and for the specific purposes specified in the Instructions, as well as to comply with Data Protection Legislation. The Processor also undertakes to continuously remain informed about applicable law in this area.

6.2 The Processor shall take measures to protect the Personal Data against all types of Processing which are incompatible with this Agreement, Instructions and Data Protection Legislation.

6.3 The Processor undertakes to ensure that all natural persons working under its management follow this Agreement and Instructions and that such natural persons are informed of the relevant legislation.

6.4 The Processor shall, at the request of the Controller, assist in ensuring that the obligations pertaining to Articles 32-36 in the GDPR are fulfilled and respond to requests for the exercise of a Data Subject's rights pertaining to the GDPR, Chapter III, taking into account the type of Processing and the information which the Processor has access to.

6.5 In the event that the Processor finds that the Instructions to be unclear, in violation of Data Protection Legislation or non-existent, and the Processor is of the opinion that new or supplementary Instructions are necessary in order to fulfil its undertakings, the Processor shall without delay inform the Controller, temporarily suspend the Processing and await new Instructions, unless the parties agree otherwise.

6.6 If the Controller provides the Processor with new or revised Instructions, the Processor shall without unnecessary delay from receipt, communicate to the Controller whether the implementation of the new Instructions causes changed costs for the Processor.

7. SECURITY MEASURES

7.1 The Processor shall take all appropriate technical and organizational security measures required pertaining to Data Protection Legislation to prevent Personal Data Breaches, by ensuring that the procedure of Processing meets the requirements of the GDPR and that the rights of the Data Subjects are protected.

7.2 The Processor shall continuously ensure that the technical and organizational security in connection with Processing is executed with an appropriate level of confidentiality, integrity, availability and resilience.

7.3 Any added or revised requirements for protective measures from the Data Controller, after the Parties have signed this Agreement, will be considered as new Instructions pertaining to this Agreement.

7.4 The Processor shall, through its control systems for authority, only grant access to the Personal Data for such natural persons working under the Processor's management and who need access to be able to perform their duties.

7.5 The Processor undertakes to continuously log access to the Personal Data in accordance with this Agreement to the extent required according to the Instructions. Logs may be erased only five (5) years after the logging event, unless otherwise stated in the Instructions. Logs will be subject to the required protection measures pertaining to Data Protection Legislation.

7.6 The Processor shall systematically test, investigate and evaluate the effectiveness of the technical and organizational measures to ensure the security of the Processing.

8. SECRECY/DUTY OF CONFIDENTIALITY

8.1 The Processor and all natural persons working under its management shall observe both confidentiality and professional secrecy during the Processing. The Personal Data may not be used or disseminated for other purposes, either directly or indirectly, unless otherwise agreed.

8.2. The Processor shall ensure that all natural persons working under its management, participating in the Processing, are bound by a confidentiality agreement pertaining to the Processing. However, this is not a requirement if they are already covered by a legally sanctioned duty of confidentiality. The Processor also undertakes to ensure that there is a nondisclosure agreement with its Sub-processor and confidentiality agreement between the Sub-processor and all natural persons working under its management, participating in the Processing.

8.3 The Processor shall promptly inform the Controller of any contacts with supervisory authorities pertaining to the Processing. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards supervisory authorities in matters relating to the Processing.

8.4 If the Data Subject, supervisory authority or third party requests information from the Processor relating to the Processing, the Processor shall inform the Controller of the matter. Information about the Processing may not be provided to the Data Subject, the supervisory authority or a third party without the written consent of the Controller, unless it is stipulated by mandatory law that information must be provided. The Processor shall assist with the communication of the information subject covered by a consent or legal requirement.

9. INSPECTION, SUPERVISION AND AUDITING

9.1 The Processor shall, without unnecessary delay, as part of its guarantees, pursuant to Article 28.1 of the GDPR, be able to report, at the request of the Controller, which technical and organizational security measures are being used for the processing to meet the requirements according to the DPA and Article 28.3.h of the GDPR.

9.2 The Processor shall at least once a year review the security of the Processing through a self-monitoring to ensure that the Processing complies with this Agreement. The result of such self-monitoring shall be communicated to the Controller upon request.

9.3 The Controller has the right to, itself or through another third party appointed by it (which may not be a competitor of the Processor), follow up that the Processor complies with the requirements of this Agreement, the Instructions and Data Protection Legislation. The Processor shall assist the Controller, or the person performing the audit on behalf of the Controller, with documentation, access to premises, IT systems and other assets needed to review the Processor's compliance with this Agreement, Instructions and Data Protection Legislation. The Controller shall ensure that personnel conducting the audit are subject to confidentiality or non-disclosure obligations pertaining to law or agreement.

9.4 Alternatively to what is stipulated in paragraphs 9.2 to 9.3, the Processor has the right to offer other ways of reviewing the Processing, such as review by an independent third party. In such a case, the Controller shall have the right, but not the obligation, to apply this alternative approach to review. In such a review, the Processor shall provide the Controller or a third party with the assistance necessary for the performance of the review.

9.5 The Processor shall provide the supervisory authority, or another authority legally entitled to do so, with the opportunity to carry out supervision in accordance with the authority's request in accordance with the legislation in force at any given time, even if such supervision would otherwise be in conflict with the provisions of this Agreement.

9.6 The Processor shall assure the Controller rights towards any Sub-processor corresponding to all of the rights of the Controller towards the Processor according to section 9 of this Agreement.

10. HANDLING OF CORRECTIONS AND DELETIONS ETC

10.1 In the event that the Controller has requested correction or deletion due to the Processor's incorrect Processing, the Processor shall take appropriate action without undue delay, at the latest within thirty (30) days from the date on which the Processor received the required information from the Controller. When the Controller has requested erasure, the Processor may only carry out Processing of the Personal Data in question as part of the process of correction or deletion.

10.2 If technical and organizational measures (e.g., upgrades or troubleshooting) are taken by the Processor in the Processing, which can have an effect on the Processing, the Processor shall inform the Controller in writing pursuant to what is stipulated about notifications in item 18 of this Agreement. The information shall be submitted in good time prior to the measures being taken.

11. PERSONAL DATA BREACHES

11.1 The Processor shall have the capability to restore accessibility and access to Personal Data within a reasonable time in the event of a physical or technical incident pertaining to Article 32.1.c of the GDPR.

11.2 The Processor undertakes, taking into account the nature of the Processing, and the information available to the Processor, to assist the Controller in fulfilling its obligations in the event of a Personal Data Breach with respect to the Processing. At the request of the Controller, the Processor shall also assist in investigating suspicions of possible unauthorized Processing and/or access to the Personal Data.

11.3 In the event of a Personal Data Breach, which the Processor has been made aware of, the Processor shall notify the Controller of the Breach in writing without unnecessary delay. The Processor shall, taking into account the type of Processing and the information available to the Processor, provide the Controller with a written description of the Personal Data Breach.

11.4. The description shall give an account of:

1. The nature of the Personal Data Breach and, if possible, the categories and number of Data Subjects affected and the categories and number of Personal Data records affected,
2. the likely impact of the Personal Data Breach, and
3. measures taken or proposed and measures to mitigate the potential negative effects of the Personal Data Breach.

11.5 If it is not possible for the Processor to provide the entire description at the same time, pursuant to paragraph 11.3 of this Agreement, the description may be provided in instalments without unnecessary further delay.

12. SUB-PROCESSOR

12.1 The Processor has the right to engage the Sub-processor(s) as set out in the attached list of Sub-processors, Annex 2.

12.2 The Processor undertakes to enter a written agreement with the Sub-processor to regulate the Processing that the Sub-processor carries out on behalf of the Controller and to only hire Sub-processors who provide adequate guarantees. The Sub-processor shall carry out appropriate technical and organizational measures to ensure that the Processing fulfils the requirements of GDPR. When it comes to data protection, such an agreement shall entail the same obligations for the Sub-processor as are set out for the Processor in this Agreement.

12.3 The Processor shall ensure in its agreement with the Sub-processor that the Controller is entitled to terminate the Sub-processor and instruct the Sub-processor to, for instance, erase or return the Personal Data if the Processor has ceased to exist in the actual or legal sense, or has entered into insolvency.

12.4 The Processor shall be fully responsible for the Sub-processor’s Processing on behalf of the Controller. The Processor shall promptly inform the Controller if the Sub-processor fails to fulfil its undertakings under the Agreement.

12.5 The Data Processor is entitled to hire new Sub-processors and replace existing Sub-processors unless otherwise stated in the Instruction.

12.6 When the Processor intends to hire a new or replace an existing Sub-Processor, the Processor shall ensure the Sub-Processor's capacity and ability to fulfil its obligations in accordance with the Data Protection Legislation. The Processor shall notify the Controller in writing of:

1. the Sub-processor’s name, corporate identity number and head office (address and country),
2. which type of data and categories of Data Subjects are being processed, and
3. where the Personal Data will be processed.

12.7 The Controller has the right to object within thirty (30) days from the date of notification pursuant to paragraph 12.6 to the Processor's use of a new Sub-processor and, in response to such objection, to terminate this Agreement to cease in accordance with what is stipulated in this Agreement, paragraph 16.4.

12.8 The Processor shall at all times maintain an accurate and up-to-date list of the Sub-processors engaged for the Processing of Personal Data on behalf of the Controller and make this list available to the Controller. The list shall, in particular, state in which country the Sub-Processor processes the Personal Data and the types of Processing that the Sub-Processor carries out.

12.9 When the Processor ceases to use a Sub-processor, the Processor shall notify the Controller of this in writing. When an agreement is terminated, the Processor shall ensure that the Sub-processor deletes or returns the Personal Data.

12.10 At the Controller’s request, the Processor shall send a copy of the agreement regulating the Sub-processor’s Processing of Personal Data in accordance with item 12.1.

13. LOCALISATION AND TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY

13.1 The Processor shall ensure that the Personal Data is handled and stored within the EU/EEA by a natural or legal person established within the EU/EEA, unless the parties to this Agreement agree otherwise.

13.2 The Processor is only entitled to transfer Personal Data to a Third Country for Processing (e.g. service, support, maintenance, development, operation or similar handling) if the Controller has given prior written consent to such transfer and issued Instructions for this purpose.

13.3 Transfer to a Third Country for Processing in accordance with this Agreement, paragraph 13.2, may only take place if it is compatible with Data Protection Legislation and meets the requirements for Processing set out in this Agreement and Instructions.

14. LIABILITY FOR DAMAGE IN CONNECTION WITH PROCESSING

14.1 In the event of compensation for damage in connection with Processing that, by confirmed judgment or settlement, shall be paid to the Data Subject due to violation of the provision of this Agreement, Instructions and/or applicable provision of Data Protection Law, Article 82 of the GDPR shall apply.

14.2 Fines pursuant to Article 83 of the GDPR, or Chapter 6, Section 2 of the Act (2018:218) containing supplementary provisions to GDPR, shall be borne by the party to the Agreement as recipient of such sanctions.

14.3 If either party becomes aware of circumstances that may result in damage to the other party, the party shall immediately inform the other party of the relationship and actively work with the other party to prevent and minimize such damage.

14.4 Notwithstanding the Main Agreement, this Agreement, paragraphs 14.1 and 14.2, prevails over other rules on the allocation between the Parties of claims among themselves with respect to the Processing.

15. CONCLUSION, TERM AND TERMINATION OF THIS AGREEMENT

15.1 This Agreement shall enter into force from the time the Agreement is signed by both Parties and until further notice. Either party has the right to terminate the Agreement with thirty (30) days’ notice.

16. AMENDMENTS AND TERMINATION WITH IMMEDIATE EFFECTS, ETC

16.1 Either party to this Agreement has the right to request renegotiation of the Agreement if the ownership of the other party changes significantly or if the applicable law, or its interpretation, changes in a way that is decisive for the Processing. Invoking renegotiation in accordance with the first sentence does not mean that the Agreement ceases to apply in any respect, but only that renegotiation of the Agreement is to be initiated.

16.2 Additions and amendments to the Agreement shall be in writing and signed by both parties.

16.3 If either party becomes aware that the other party is acting in violation of the Agreement and/or Instructions, the first party shall inform the other party without delay of the actions in question. The party is then entitled to suspend the performance of its obligations pursuant to the Agreement until such time as the other party has declared that the actions have ceased, and the explanation has been accepted by the party that made the complaint.

16.4 If the Controller objects to the Processor's use of a new Sub-processor, pursuant to this Agreement, paragraph 12.7, the Controller has the right to terminate the Agreement with immediate effect.

17. MEASURES IN THE EVENT OF TERMINATION OF THE AGREEMENT

17.1 Upon termination of the Agreement, the Processor shall, without undue delay, depending on the Controller's choice, either delete and certify to the Controller that it has been performed, or return

1. all Personal Data Processed on behalf of the Controller; and
2. all related information such as Logs, Instructions, system solutions, descriptions and other documents obtained by the Processor through information exchange under the Agreement.

17.2. In connection with the return of data, the Processor shall also delete existing copies of Personal Data and associated information.

17.3 The obligation to delete or return Personal Data and/or associated information does not apply if the storage of Personal Data or the information is required under Union or relevant national law where Processing may be carried out pursuant to the Agreement.

17.4 If Personal Data or related information is returned, it shall be in a commonly used and standardized format, unless the parties have agreed on another format.

17.5 Until the data is deleted or returned, the Processor shall ensure compliance with the Agreement.

17.6 Return or deletion pertaining to the Agreement shall be carried out no later than thirty (30) calendar days counting from the time of termination of the Agreement, unless otherwise stated in the Instructions. Processing of Personal Data which the Processor subsequently carried out shall be regarded as unauthorized Processing

17.7 Provisions on confidentiality/professional secrecy in Section 8 shall continue to apply even if the Agreement otherwise ceases to apply.

18. NOTIFICATIONS WITHIN THE PURVIEW OF THIS AGREEMENT AND INSTRUCTIONS

18.1 Notifications about the Agreement and its administration, including termination, shall be submitted via email or in any other manner agreed by the Parties to each Party's contact person for the Agreement.

18.2 Notifications about the collaboration of the Parties regarding the data protection shall be submitted via email or in any other manner agreed by the Parties to each Party's contact for the Parties' cooperation on data protection.

18.3 A notification shall be deemed to have been received by the recipient no later than one (1) business day after the notification has been sent.

19. CONTACT PERSONS

19.1 The Parties shall each appoint a contact person for the Agreement.

19.2 The Parties shall each appoint a contact person for their cooperation on data protection.

20. RESPONSIBILITY FOR INFORMATION REGARDING PARTIES, CONTACT PERSONS AND CONTACT INFORMATION

20.1 Each party is responsible for ensuring that the information specified in Section 1 of the Agreement is always up-to-date and accurate.

20.2 Any change to the information in Section 1 shall be notified to the counterparty in accordance with paragraph 18.1 of the Agreement.

21. CHOICE OF LAW AND DISPUTES

21.1 When interpreting and applying the Agreement, Swedish law shall apply with the exception of the choice of law rules. Disputes regarding the Agreement shall be settled by a competent Swedish court.

22. THE PARTIES’ SIGNATURES ON THE AGREEMENT

22.1 This Agreement is provided either in digital format for electronic signature or in paper format for self-signing. In the latter case, the contract is drawn up in two identical copies, each of which is given to the parties.

22.2 If the Agreement is signed electronically, the signature page is disregarded.

Controller Processor

Mid Sweden University *[Insert the full name of the organization]*

Place and date: Place and date:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name clarification Name clarification

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Signature Signature

Annex 1 – Instructions for the Processing of Personal Data

[Yellow highlighted text within square brackets is to be deleted before the contract is drawn up.]

In addition to what is already stated in the Data Processing Agreement, the Processor shall also follow the following Instructions:

|  |
| --- |
| 1. Purpose, object and nature |
| [Insert the main purpose of the Processor's Processing of Personal Data. Indicate what the Processor provides and what the purpose of this is. Why is the Processing carried out? What is the purpose? The description should be so complete that anyone should be able to understand the content and why a Data Processing Agreement has been drawn up. One tip is to formulate the purpose as if you are writing an ad. Example: Provision of an HR tool for the purpose of administering the payment of salaries, or, the provision of a cloud computing service for the purpose of storing information in a secure manner.]The Controller has instructed the Processor to:  |
| 2. The Processing includes the following types of Personal Data |
| [Specify a list of the types of Personal Data that the Processor is entitled to process. Example: Name, e-mail address, postal address, telephone number, social security number, employee ID, study ID, pictures, audio recordings, videos, salary information, personality tests, research ID or other type of encoded data, etc. This is all kinds of information that can be directly or indirectly linked to a living person.Certain personal data are by their nature particularly sensitive and therefore require stronger protection (sensitive personal data). Indicate if any of the following categories are addressed: ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health data, a person's sex life or sexual orientation, genetic data or biometric data.] The Personal Data that will be Processed are:  |
| 3. Processing covers certain categories of Data Subjects  |
| [Compile a detailed list of the different categories of individuals whose Personal Data will be Processed. Example: employees, consultants, students, research participants, job seekers, guardians, trainees, children, patients, etc.] The Processing includes the following categories of Data Subjects:  |
| 4. Specify special requirement when it comes to Processing of Personal Data carried out by the Processor  |
| [Specify which specific requirements the Processor must take into account. This may, for example, involve logging or whether the data is to be returned in any special way, etc. Below are specific requirements that are common and therefore specified in advance. If the requirements are not relevant to the specific Processing, they may be removed.] Example: When Processing Sensitive Personal Data, it shall be encrypted. Example: The Processor may not export or otherwise retrieve or Process the Controller's Personal Data that is Processed in the Service and/or on behalf of the Controller, in order to then use the Personal Data and/or other type of data for its own use in the Processor's activities. In cases where the Processor wishes to use the data that emerges in connection with the Processing, the Processor may request this information as a request for public documents. All information requested shall be subject to a confidentiality and security assessment and may only be disclosed after this assessment has been carried out and provided that there is no confidentiality.  |
| 5. Specify specific technical and organizational security measures regarding the Processing of Personal Data by the Processor  |
| [Specify the technical and organizational security measures to be taken for the Processing. Any reference may be made to one or more annexes, if any. Most often, a dialogue needs to be conducted with the Processor to investigate which security measures become applicable. Examples of specific requirements that are common are given below.]The Processor shall take the following security measures when Processing Personal Data: Organizational security measures: [May relate, for example, to establishment governing documents for the Processing, allocation of responsibilities, assignment of authorization, risk and incident management, follow-up, investigation of unauthorized access, etc.]. Personal security measures: [For example, training for handling tasks, routines for remote work, etc.]. Physical security measures: [For example, monitoring of premises, location and protection of hardware, equipment requirements, entry requirements, access protection, destruction of physical storage media, etc.]Technical security measures: [For example, encryption, pseudonymization of data, system monitoring, logging, backup, technical authentication, requirements for data communication, requirements for access for repair and service, etc.]. Example: Especially when accessing remotely: The Controller and the Processor shall ensure that Personal Data is not Processed in a way that does not allow traceability, such as screen sharing. The Controller is responsible for Logging in its own environment when connected remotely. In cases where the Processor retrieves Personal Data for Processing outside the Controller's infrastructure in the event of a remote connection, the Processing shall be logged. The Logs shall indicate which measures have been taken and which Personal Data it relates to. It must also be clear when the measure has been taken and by whom.  |
| 6. Specify specific requirements for Logging with regard to the Processing of Personal Data and who should have access to it |
| [Describe whether the Processing carried out by the Processor shall be Logged, and if so, how the Logging shall take place. The following are specific requirements for Logging that are common and therefore pre-specified. If the descriptions are not relevant to the specific Processing, they may be removed.]Example: Access to Personal Data shall be possible to follow up afterwards through Log or similar documentation. When handling Personal Data, traceability shall be provided regarding who processed the data, the time, what data was the subject of the Processing and what the Processing consisted of. Logs must show the history of the change of notes and who implemented the change. The documentation shall be able to be checked by the Processor and shall be able to be reported back to the Controller.  |
| 7. Location and Transfer of Personal Data to Third Countries  |
| Option 1 (recommended): Personal data may only be Processed within the EU/EEA and within a country that has received an approved and valid adequacy decision from the European Commission. Option 2: For the transfer of Personal Data to a Third Country, the EU Commission's standard contractual clauses shall be drawn up between the Controller and the Processor. The following additional security measures shall be implemented at the time of transfer: * [Insert additional security measures, such as encryption, pseudonymization, etc.]
 |
| 8. Other Instructions regarding Processing of Personal Data carried out by the Processor |
| [If required, add additional Instructions for the Processor's Processing of Personal Data, in addition to what is already stated above. For example, it may be information that has not fit in elsewhere, or boundaries to clarify what the Processor may and may not do.]The following other Instructions apply to the Processing of Personal Data: * Option 1: [Indicate which other Instructions apply.]
* Option 2: No other instructions.
 |

Annex 2 – List of approved Sub-processors

[Yellow highlighted text within square brackets is to be deleted before the contract is drawn up.]

The Controller approves the hiring of the Sub-processor below by the Processor for the Processing of Personal Data.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Organization | Address and contact details | Location of Personal Data (country) | Types of Personal Data | Purpose of Processing by the Sub-Processor | Safeguard mechanism for possible transfer to Third Countries |
| [Insert name and organization number of the organization hired] | [Insert the address of the Sub-processor and the e-mail address of the contact person] | [Insert where the Sub-processor Processes Personal Data] | [Insert the Types of Personal Data Processed by the Sub-processor] | [Specify the purpose of the Processing by the Sub-processor] | [Insert whether a transfer to a third country takes place and, if so, what safeguard mechanism is used] |
| [Insert name and organization number of the organization hired] | [Insert the address of the Sub-processor and the e-mail address of the contact person] | [Insert where the Sub-processor Processes Personal Data] | [Insert the Types of Personal Data Processed by the Sub-processor] | [Specify the purpose of the Processing by the Sub-processor] | [Insert whether a transfer to a third country takes place and, if so, what safeguard mechanism is used]  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

1. The General Data Protection Regulation EU 2016/679 stipulates that there must be a written agreement on the Processor's Processing of Personal Data on behalf of the Controller. [↑](#footnote-ref-2)