| **[Faculty/Department/Collaborative centre]** | **Agreement** SLU ID: SLU.[Write number here]DD MMMM 20YY |
| --- | --- |

Data processing agreement

## Parties

1. THE SWEDISH UNIVERSITY OF AGRICULTURAL SCIENCES, registration number 202100-2817, address (**Data Controller**)
2. Counterpart, registration number, address, (**Data Processor**)

# Background and purpose

* 1. This data processing agreement (‘Processing Agreement’) is an annex to [refer to title of main agreement/Write the title of the agreement to which this data processing agreement is annexed](‘Agreement’)
	2. The Processing Agreement aims to regulate how the Data Processor processes personal data on behalf of the Data Controller. The Processing Agreement has been created following the requirements in the EU’s General Data Protection Regulation (EU) 2016/679 (GDPR), however it can also be adjusted as needed and used for data processing regulated by other data protection legislation.
	3. Instructions for the Processing Agreement (Annex 1) are to be completed by the Parties in order to meet the requirements in the GDPR and other legal provisions applicable to the processing of personal data.

# Processing

* 1. The Data Processor accepts that personal data will only be processed in accordance with (i) this Processing Agreement, (ii) the Data Controller’s documented instructions, and (iii) data protection legislation.
	2. Annex 1 contains more detailed instructions for the Data Processor from the Data Controller on the way personal data is to be processed within the framework of this Processing Agreement. The Data Controller may change or issue additional written instructions to the extent necessary for ensuring data processing complies with the law, or so the Data Processor is able to process data in accordance with the Contract.

# The Data Controller’s responsibilities

* 1. The Data Controller agrees to ensure that there is a legal basis for the processing of personal data the Data Processor is carrying out in accordance with this Processing Agreement.
	2. The Data Controller agrees to notify the Data Processor without undue delay of any new circumstances or information that may affect the Data Processor’s obligations as per this Processing Agreement or data protection legislation.

# The Data Processor’s general obligations

* 1. The Data Processor must restrict access to personal data and ensure that access to the personal data is only granted to those who require it for performing the tasks stipulated in the Agreement or this Processing Agreement.
	2. The Data Processor agrees that they will not share any of the personal data under this Processing Agreement with a third party without the permission of the Data Controller.
	3. The Data Processor agrees to ensure that those working under their management comply with what is stipulated in this Processing Agreement and at any given time, other instructions that may be issued by the Data Controller. Those working under the Data Processor’s management must be informed about the relevant data protection legislation. The Data Processor must immediately notify the Data Controller and await new instructions if the Data Processor believes they lack instructions or those they have received are unclear or are in breach of data protection legislation.
	4. Upon request of the Data Controller, the Data Processor must assist the Data Controller with data protection impact assessments and prior consultation with the supervisory authority.
	5. The Data Processor must inform the Data Controller, without undue delay, of any contacts with the relevant supervisory authority that may be significant to the personal data processing. The Data Processor may not represent the Data Controller, or act on their behalf in contact with the relevant supervisory authority or other third party.

# Security measures and mechanisms

* 1. The Data Processor must take the measures required to comply with Article 32 of the GDPR and other suitable technical and organisational measures stipulated in other data protection legislation. Hence, the Data Processor must establish a level of security that is suitable in relation to the risk processing entails, paying particular attention to the risk of accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to the data being processed. The Data Processor must, at any given time, document the security measures taken. Upon request of the Data Controller, the Data Processor must, without undue delay, provide the Data Controller with an account of the security measures taken. The Data Controller may always require that the Data Processor takes further security measures if required in order to comply with data protection legislation.
	2. The Data Processor must take suitable technical and organisational measures to assist the Data Controller in fulfilling the rights of data subjects in accordance with Chapter 3 of the GDPR.

# Personal data breaches

* 1. In the event of a personal data breach, the Data Processor must assist the Data Controller in fulfilling their obligations. The Data Processor must provide support to investigate suspicions of unauthorised processing or access to personal data.
	2. Following personal data breaches, or if there is a risk of a personal data breach, the Data Processor must notify the Data Controller of the incident in writing, without undue delay. The Data Processor must provide the Data Controller with a written description of the personal data breach. The description must include details such as:
		1. the nature of the personal data breach, the time of its detection and, if possible, the time when the breach occurred; the categories and number of data subjects affected and the number of personal data records concerned;
		2. the name and contact details of the Data Processor’s data protection officer or other contact details of a person at the Data Processor’s organisation where more information can be obtained;
		3. the likely consequences of the personal data breach, and
		4. the measures taken or proposed and the measures taken to mitigate the possible adverse effects of the personal data breach.

# Sub-processor

* 1. The Data Processor is not permitted to engage a sub-processor for processing personal data without obtaining prior written authorisation from the Data Controller.
	2. In cases where the Data Processor has received prior written authorisation from the Data Controller to engage a sub-processor to perform a specific processing operation, the sub-processor must be contractually bound by the same obligations when processing personal data as the Data Processor must follow under the Processing Agreement. The sub-processor must especially provide sufficient guarantees to implement suitable technical and organisational measures in such a way that the data processing complies with the requirements of data protection legislation.
	3. If the sub-processor does not fulfil their obligations regarding personal data processing, the Data Processor will be held fully responsible by the Data Controller for the performance of the sub-processor’s obligations.

# Terminating processing

* 1. As part of the fulfilment of Point 6.2 above, the Data Processor must erase or rectify incorrect or incomplete personal data following instruction from the Data Controller. Following the Data Controller’s instruction to erase the personal data, the Data Processor may only process this data as part of its erasure and must undertake the measure without undue delay, however no later than thirty (30) days from the time of the request.
	2. Upon termination of this Processing Agreement, the Data Processor must, as instructed by the Data Controller, (i) transfer all personal data to the Data Controller using an agreed standardised or open format, or (ii) erase all personal data. Following transfer of the personal data, the Data Processor must erase the personal data. The transfer must take place promptly following instruction from the Data Controller, and within a maximum of ten (10) days. Erasure of personal data must take place without undue delay and no later than thirty (30) days from the time of instruction, or after the transfer of personal data is complete.

# Confidentiality

When processing personal data, the Data Processor must observe both professional secrecy and confidentiality, meaning that personal data or details about the processing thereof may not be disclosed to unauthorised third parties. The Data Processor must also ensure that those who are able to access the personal data as part of the Data Processor’s fulfilment of their obligations under this Processing Agreement enter into a confidentiality agreement imposing the same obligations as stipulated above in Point 7.

# Damage liability

The Data Processor must compensate and indemnify the Data Controller for all claims, costs, damages and losses caused by the Data Processor’s incorrect processing. The Data Processor must also compensate the Data Controller for any damages to individuals and administrative fines stipulated in the GDPR incurred following incorrect processing. Similarly, the Data Processor must cover any reasonable costs that are the result of the Data Controller needing to defend itself against claims from third parties and/or actions imposed by the supervisory authority. Incorrect processing refers to processing that contravenes the GDPR, the Agreement, this Processing Agreement or instructions from the Data Controller.

# Miscellaneous

* 1. The parties must jointly ensure that the instructions that apply at any given time are provided in Annex 1.
	2. Additions and changes to this Processing Agreement must, in order to be valid, be in writing and signed by authorised representatives for both parties. However, the Data Controller may change the instructions in Annex 1 at any given time, in accordance with what is stated in Point 3.2 of this Processing Agreement.

The Data Processor may not delegate the obligations in this Processing Agreement to third parties without the written consent of the Data Controller.

# Valid until

* 1. Provisions regarding the termination of the Processing Agreement are stipulated in the Agreement.
	2. This Processing Agreement is valid starting the date it is signed and for as long as the Data Processor continues to process the Data Controller’s personal data under the Agreement, and for the subsequent period necessary for the Data Processor to fulfil its remaining obligations as per the Processing Agreement.

# Dispute resolution

Any disputes regarding the interpretation or application of this Processing Agreement are to be settled in accordance with the provisions on dispute resolution in the Agreement.

This Processing Agreement is governed by Swedish substantive law, disregarding its conflict-of-law rules.

This Processing Agreement has been drawn up in duplicate, with each party holding one original.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Town/city and Date Town/city and Date

Swedish University of Agricultural Sciences XXX AB

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
Signature Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
N.N./Title Print name/Title
Division/Department of Xxx

(Same person eligible to
sign Agreement).

# ANNEX 1INSTRUCTIONS FOR DATA PROCESSORS

This document forms the Data Controller’s instructions for the Data Processor.

## Why the data is being processed (Data Processor’s purpose)

|  |
| --- |
| * [Describe the reasons why the Personal Data is being processed, and link this to the service being provided by the Data Processor to ensure that the Personal Data is only processed to the extent necessary for the task.]
 |

## Categories of data subjects

|  |
| --- |
| * [State the categories to which the Personal Data belongs, e.g. patients, students or employees]
 |

## Personal data

|  |
| --- |
| [State the Personal Data being processed, e.g. name, personal identity number, telephone number or address.] |

## Sensitive personal data (where applicable)

|  |
| --- |
| [State the type of sensitive Personal Data being processed.] |

## Special security measures

|  |
| --- |
| * [State the special technical and organisational measures taken when the Pesonal Data is processed by the Data Processor.]
 |

## Terminating processing

|  |
| --- |
| * [State the option that will apply when Personal Data is either transferred or erased once the Agreement is terminated, see Point 8.2]
 |

## Processing with the help of a sub-processor

Select one of the options below.

 Option 1: These instructions prohibit the Data Processor from engaging another data processor (sub-processor).

Option 2: The Data Processor may only engage another Data Processor if a written agreement has been obtained from the Data Controller.

Option 3: The Data Processor is generally entitled to engage a new data processor (sub-processor) that adheres to data protection legislation and what is stipulated in the Processing Agreement. However, a new sub-processor may only be engaged once the Data Controller has been notified of any such plans, and has been given the opportunity to object, within reasonable time, to this choice.

X

## Processing of personal data within Sweden, the EU/EEA and third countries.

Select one of the options below.

Option 1: Personal data may only be processed in Sweden.

Al Option 2: Personal data may be processed within the EU/EEA.

X

Option 3: Personal data may be processed within the EU/EEA and may be transferred to and processed in a third country, territory, sector of a third country and within an international organisation that at any given time has a valid adequacy decision from the European Commission.

*Processing of personal data in a third country or international organisation without a valid adequacy decision*

Personal data may be transferred and processed in the third country or international organisation listed below without there being an adequacy decision based on the legal solution and possible safeguards stated below. Safeguards refers to actions that ensure that transfer and subsequent processing of personal data comply with Chapter 5 of the GDPR.

|  |  |  |
| --- | --- | --- |
| **Third country or international organisation** | **Legal solution** | **Safeguards (if necessary, add an annex)** |
| [Name] | [State legal solution.] | [Describe safeguard(s) to ensure transfer complies with Chapter 5 of the GDPR.] |
|  |  |  |
|  |  |  |
|  |  |  |

## Authorised sub-processors

|  |  |  |
| --- | --- | --- |
| **Sub-processor** | **Processing description** | **Country** |
| [Name] | Describe how the sub-processor will process Personal Data | [State where the processing will take place.] |
|  |  |  |
|  |  |  |
|  |  |  |