# Joint Controllership Agreement

# Parties

1. Uppsala universitet, for the purpose of this Agreement acting through its [department], org. reg. no. 202100-2932, [address] (below “**UU**”);

and

1. [Name], org. reg. no. […], [address] (below “[**…**]”)

have on this date entered into the following agreement on joint controllership when processing certain personal data (“**the** **Agreement**”).

 UU and […] are referred to below collectively as “the Parties” and individually as “the Party”.

# Background and purpose

The Parties have entered into an agreement concerning [xxxx] (“**the** **Main Agreement**”). To fulfil their commitments in line with the Main Agreement, the Parties will process personal data. This Agreement is to ensure that the Personal Data to be processed in line with the Main Agreement is handled in accordance with the requirements of the General Data Protection Regulation (GDPR), other applicable legislation and established standards, and that the Personal Data is not made accessible to unauthorised persons.

The Parties acknowledge that they are jointly responsible for the Processing of the Personal Data that takes place within the framework of the Main Agreement and that the Agreement covers all such Processing of Personal Data.

# Definitions

This Agreement uses the corresponding definitions found in Article 4 of GDPR, which include the following.

‘**Processing**’ (or ‘**Process**’) means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The ‘**General Data Protection Regulation’** refers to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (EUT 119, 4.5.2016, p. 1).

**‘Sensitive Personal Data’** refers to Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership and Processing of genetic data, biometric data to uniquely identify a natural person, data on health or data on a natural person's sexual life or sexual orientation.

**‘Personal data’** means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

‘**Controller**’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**‘Processor’** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

‘**Personal data breach**’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

‘**Data subject’** means the person to whom the Personal Data refers.

# Documents in the Agreement

This Agreement consists of this document, including **Appendix 1** and **Appendix 2.**

# General commitments of the Parties

* 1. The Parties are responsible for ensuring that the Processing of Personal Data carried out by each Party within the framework of this Agreement complies with GDPR and other applicable legislation.
	2. The Parties are both individually and jointly responsible for ensuring there is a lawful basis for the Processing and that the Personal Data is not Processed in a way that extends beyond the purpose of the Processing.
	3. If Processing is likely to lead to a high risk for the Data Subjects, the Parties are responsible for carrying out an impact assessment in accordance with Article 35 of GDPR.
	4. The Parties are to limit access to the Personal Data exclusively to those staff at the Party who need the Personal Data to fulfil their obligations in accordance with the Main Agreement and this Agreement.
	5. The Parties must take appropriate technical and organisational protective measures to ensure that the rights of the Data Subjects are protected. The Parties are responsible for continuously evaluating and updating the Processing and its protective measures. The Parties are responsible for the Processing being conducted in accordance with the security standard set out in Appendix 2.
	6. The Party that collects the Personal Data is responsible for informing the Data Subjects about the Processing. This obligation also means that general information about the content of this Agreement must be included in the information supplied to the Data Subjects.
	7. The Parties must take necessary measures to safeguard the interests of the Data Subjects and the rights that follow from GDPR and other applicable legislation.

# Processor

6.1 The Party may engage a Processor to process Personal Data within the framework of this Agreement. When Personal Data is processed by a Processor, the process must be regulated by a processor agreement in accordance with Article 28 of GDPR.

6.2 The Party that engages a Processor must inform the other Party thereof and is responsible towards the other Party for the transfer to/from and the Processor's Processing of the Personal Data.

# Transfer of Personal Data to third countries

7.1 Any transfer to a third country assumes that the requirements and measures that follow from GDPR have been met.

7.2 The Parties are in agreement that a transfer of Personal Data to a third country requires all Parties’ written consent.

# Personal Data Breach

8.1 The Parties are responsible for taking immediate and reasonable measures to limit any damage resulting from a Personal Data Breach.

8.2 The Parties are responsible for informing each other in a timely manner of any Personal Data Breach. The information must as a minimum contain:

a) the nature of the Personal Data Breach, including, if possible, the categories of and approximate number of Data Subjects affected and the categories of and approximate number of Personal Data records affected;

b) the name and contact details of the data protection officer or other contact point where more information can be obtained;

c) the likely consequences of the Personal Data Breach; and

d) the measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

8.3 The Parties agree to assist each other, where necessary, with reasonable support so that the handling of Personal Data Breaches complies with GDPR and other applicable legislation.

8.4 The Parties have a joint responsibility to report a Personal Data Breach to the supervisory authority and, if required/necessary, to inform the Data Subject concerned. The Parties agree that such a notification will be made by [specify Party] in the event of a Personal Data Breach.

# Contact

9.1 The Parties have a joint responsibility to ensure that the Data Subject's rights are met in accordance with GDPR and other applicable legislation. The Parties are thus in agreement that a Data Subject can contact either Party. For this Agreement, [specify Party] will be the joint point of contact for Data Subjects and the supervisory authority.

9.2 The Parties are to notify the other Party without delay of any contact with Data Subjects which is of relevance for the Processing of Personal Data.

9.3 The Parties agree to assist each other, at the request of either Party, with handling a Data Subject's request to exercise their rights under GDPR. Support must be provided without undue delay.

9.4 The Parties are to notify the other Party without delay if one Party discovers that the Processing of Personal Data under this Agreement is not covered by specific regulations of this Agreement.

9.5 The contact person for each Party and each Party’s Data Protection Officer is:

 Contact person at UU: [Name and email],

 Data Protection Officer: dataskyddsombud@uu.se

 Contact person at […]: [Name and email]

 Data Protection Officer: [Email]

# Liability

10.1 In cases where Data Subjects make a claim for compensation against one of the Parties due to material or non-material damage as a result of a violation of GDPR, Article 82 of GDPR is to apply. This specifies that the Parties are jointly and severally liable. However, a Party has the right to recover from the other Party any part of the compensation that corresponds to the other Party's responsibility for the damage suffered.

10.2 The Parties agree that administrative fines under Article 83 of GDPR or any applicable national GDPR implementation legislation will be borne by the Party on which such a fee has been imposed.

# Changes and amendments

11.1 Changes and amendments to this Agreement must be made in writing and signed by the Parties in order to be valid.

11.2 Beyond what is specifically stated in this Agreement, neither Party has the right to fully or partially transfer the rights or obligations under this Agreement without the written consent of the other Party.

# Term of the Agreement and termination

12.1 This Agreement applies from the time that both Parties sign the Agreement and as long as there is joint controllership between the Parties for the Personal Data.

12.2 Unless the Parties agree otherwise or applicable legislation states otherwise, the Party that is no longer responsible for the Personal Data upon termination of the Agreement shall delete that Personal Data or transfer it to the Party considered solely responsible for it.

12.3 In the event that either Party is obliged by primary or secondary legislation, agency regulations or decisions to retain Personal Data even after this Agreement has ceased to apply, this Personal Data may only be used for the purpose stated in the legislation, agency regulations or decisions that cause the Personal Data to be retained. In that case, the other Party must be informed of this and the reasons for it.

# Applicable law and disputes

13.1 Unless otherwise stated in the Main Agreement, disputes regarding the interpretation or application of this Agreement are to be settled according to Swedish law and brought before an ordinary Swedish court. [In the event that Parties are Swedish authorities, the dispute is to be ultimately settled instead by the immediately higher authority or otherwise by the applicable dispute resolution mechanism of the Swedish state.]

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

This Agreement has been drawn up in 2 (two) identical copies, of which each Party has received one copy.

**Uppsala universitet [**Name]

*Signature Signature*

*Name in block letters, position Name in block letters, position*

*Place and date Place and date*

Appendix 1 – Personal Data Processing of the Parties

The Parties have specified below the aspects covered by Processing in the Agreement

1. **Purpose of Processing**

The purpose of Processing Personal Data is (*why the Personal Data is being Processed, e.g. joint research project, etc*.)

1. **Lawful basis for Processing**

The Parties agree that the lawful basis for Processing is (*e.g. exercise of official authority and a matter in the public interest*).

1. **Data Subject categories**

The categories of Data Subject affected are: (*which groups of residents are Processed in the system, e.g. municipal residents, pensioners, savers, students, employees within the organisation, elected representatives, individuals receiving a service, research staff, etc.*)

1. **The types of Personal Data being Processed**

The Personal Data being processed is of the following types: (*e.g. name, IP address, email address, property reference, sole tradership, etc.*)

1. **Sensitive Personal Data (where applicable)**

The Sensitive Personal Data affected by the Processing is: (*e.g. racial or ethnic origin, political opinions, religious or philosophical beliefs, health and medical data, trade union membership and Processing of genetic and biometric data. When Processing Sensitive Personal Data, special consideration must be given to handling the data in a particular manner in accordance with the Swedish Tax Agency's guidance for classified Personal Data within public administration.).*

1. **Processing**

The Personal Data will be Processed in the following manner (*cf. point 3 of the Agreement, such as who is responsible for the collection, registration, organisation, storage, processing, dissemination or other provision of data, compilation or collation. Don’t forget that if Sensitive Personal Data is Processed, it must be listed here as "Processing of Sensitive Personal Data"*).

1. **Specific conditions concerning Processing:**

(*State whether there is anything specific that the Parties must take into account when processing the Personal Data.)*)

1. **Processing in third countries (where applicable)**

(*State whether the Personal Data will be transferred, directly or indirectly, to countries outside the EU/EEA.)*)

1. **Termination procedures**

See point 12 of the Agreement.

1. **Information about the Processor**

(*State any Processors below.*)

|  |  |  |
| --- | --- | --- |
| **Name of Processor** | **Type of Processing and reasons for Processing** | **Location of Processing and, if outside EU/EEA, lawful basis for transferring Personal Data** |
|  |  |  |
|  |  |  |

Appendix 2 – Information security

[When Processing, the Personal Data must be protected by information security measures that ensure a relevant level of security based on the sensitivity of the information.

For questions regarding the content of Appendix 2, please contact the Security and Safety Division, Information Security Unit.]

The Parties have carried out information classification and an analysis based on information security requirements according to the Swedish and international standard SS-ISO/IEC 27001.

The Parties guarantee that

* Information security measures are conducted in accordance with ISO/IEC 27001 or equivalent for this area.
* The Parties' information systems/IT services are developed to meet information security needs, i.e. confidentiality, accuracy and availability requirements.
* The following aspects are fundamental to the Parties' management of information security: access restriction, accuracy, traceability and availability.
* External protection of the Parties’ premises is in place in the form of locks and alarms. Procedures are in place for the allocation and management of equipment and authorisations, and these are reviewed regularly.
* Safeguard mechanisms in the form of a firewall are in place.
* Only authorised personnel have access to the Parties’ IT environment.
* The Parties have administrative procedures and technical measures in place to distinguish information from different customers.
* The Parties work in line with implemented information security management systems which regulate the follow-up of IT security breaches.
* The Parties will report any Personal Data Breaches that affect the Parties’ data in the course of their work in accordance with the contact information received.