# **Personal Data Processing Agreement**

## Parties

1. Uppsala University**, [**name of the unit**],** (hereafter referred to as the “**Controller**”), corporate identification number [number], [address]; and
2. **[**processor name], (hereafter referred to as the “**Processor**”), corporate registration number [number], [address];

have on the day of last signature below entered the following personal data processing agreement (the “**Agreement**”). The parties set out in a) and b) above are each a **Party** and collectively the **Parties** below.

## Background and Purpose

This Agreement shall ensure that the Personal Data covered by the Processor’s Processing is managed in accordance with the requirements pursuant to the General Data Protection Regulation, other applicable legislation and established standards and that the Personal Data does not become accessible to unauthorised persons.

The Parties have entered into an agreement regarding [reference to agreement] (the “**Main Agreement**”).

This Agreement aims to meet the requirements of applicable personal data laws including the GDPR, which require a written Agreement regarding the Processor’s Processing of the Personal Data on behalf of the Controller.

## Definitions

This Agreement has definitions equivalent to those in Art 4 of the GDPR, which among other things entails 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** (“**GDPR**”)refers to the 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 (EUT 119, 4.5.2016, p. 1).

**Personal Data** means any information relating to an identified or identifiable natural person; 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.

**Personal Data 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. If the purposes and means of such Processing are determined by Union or Member State law, the Personal Data Controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**Personal Data Processor** means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Personal Data 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** refers to the person to which the Personal Data relates.

## The Agreement’s Agreement Documents

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

## Processing Covered by the Agreement

5.1 Specified instructions to the Processor regarding its Processing of Personal Data within the scope of this Agreement are set out in **Appendix 1**. The Parties agree that the Controller can change or issue further written instructions to the extent necessary to secure that the Processing is lawful and/or to assure that the Processing according to Section 2 of this Agreement is possible and that the Processor is obligated to conform to such changed or further instructions. It is the responsibility of the Controller that **Appendix 1** correspond to the instructions in force at any time.

5.2 The *Processors measures for information security in relation to the Processing* covering the Processing according to this Agreement is specified in **Appendix 2**. The Processor shall not relinquish from any of the measures in **Appendix 2** without a written permission from the Controller. It is the responsibility of the Parties that **Appendix 2** correspond to the measures for information security in force at any time.

## Processing of Personal Data

6.1 The Processor hereby undertakes to Process Personal Data in accordance with GDPR, this Agreement and at each time applicable written instructions from the Controller, attributable to this Agreement.

6.2 The Controller solely decides on the purpose of and the means for the Processing of Personal Data that the Processor carries out on behalf of the Controller.

6.3. The Processor may not Process Personal Data for any other purpose or in any way other than absolutely necessary at each Processing occasion in order to fulfil its undertakings under this Agreement or for any other measure which the Controller specifically permits in writing.

## The Personal Data Processor’s Primary Obligations

7.1 The Processor guarantees that it possesses necessary capacity and ability to fulfil its obligations under this Agreement and applicable data protection legislation, and that it implements such appropriate technical and organisational measures on an ongoing basis, as required to ensure that the Data Subject’s rights are protected.

7.2 If the Processor lacks instructions that the Processor deems necessary to perform the assignment, the Processor shall inform the Controller without delay of its position and await instructions from the Controller.

7.3 The Processor shall without delay inform the Controller of any contacts from a regulatory authority that concern or may be of significance to the Processing of the Personal Data. The Processor does not have the right to represent the Controller or act on behalf of the Controller towards a regulatory authority or another third party.

7.4 If the Data Subject, a regulatory authority or any other third party requests information from the Processor that concerns Processed Personal Data, the Processor shall refer such person to the Controller. The Controller and the Processor shall thereafter agree on a suitable approach for the release of the requested information.

7.5 The Processor shall, when necessary, assist the Controller to meet a request for correction, blocking or deletion of the Personal Data presented by the Data Subject. Such aid shall be provided without undue delay and in any event within such time so that the Controller may meet the request by the Data Subject within the time limit stipulated by GDPR (one month with the possibility to prolongation by two month if deemed necessary by the Controller taking into account the complexity or volume of the request).

7.6 The Processor shall notify the Controller without undue delay when becoming aware of a Personal Data Breach.

7.7 The Controller has the right by itself or through a third party to verify that the Processor complies with its obligations under in this Agreement and the instructions issued by the Controller. The Processor shall, at its own expense and within what is legally possible, make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this Agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

7.8 The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes GDPR or other applicable data protection legislation.

7.9 Information in the service’s log may only be used by the Processor to maintain or improve the service’s functionality and quality. The Controller has the right to study the information Registered in the log.

## Confidentiality and Professional Secrecy

8.1 The Personal Data is subject to confidentiality. Unless otherwise provided by mandatory law, the Processor, its employees or sub-processors may not disclose any of the Personal Data to a third party without first having obtained the Controller’s consent.

8.2 The Processor is responsible for engaged personnel being informed of and observing applicable confidentiality. If the Controller so desires, a separate confidentiality agreement shall be signed by engaged personnel.

1. Sub-Processor

9.1 The Processor may not engage any sub-processor without having obtained a specific written consent from the Controller in advance. Such engagement may only take place by written agreement with the sub-processor. According to the sub-Agreement, the same obligations as are incumbent on the Processor under this Agreement shall be incumbent on the sub-processor and above all, the sub-processor shall provide adequate guarantees to implement appropriate technical and organisational measures so that the Processing meets the requirements of the GDPR.

9.2 If the sub-processor does not fulfil its obligations regarding the Processing of the Personal Data, the Processor is fully liable towards the Controller.

9.3 In order for the Controller to be able to fulfil its statutory obligations as a Personal Data Controller, all sub-processors must be known by and reported to the Controller as well as the purpose of engaging the sub-processor for the Processing. The Controller shall also be informed of the country in which the Processing takes place and, if it is a non-EU/EEA country, the lawful basis for the transfer of the Personal Data to that country.

1. Security Measures

10.1 The Processor shall implement appropriate technical and organisational measures in order to ensure and be able to demonstrate that the Processing is done in accordance with the GDPR and ensure that the rights of the Data Subject are protected against, among other things, unauthorised access, destruction and modification. The Processor shall further observe instructions and other regulations issued by any regulatory authority relating to the Processing.

10.2 Accordingly to GDPR Art 32 and taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of the Processing as well as its risks, the Parties individually and in consultation are responsible for implementing appropriate technical and organisational measures, designed for data protection by design and by default in accordance with applicable data protection legislation.

1. Notification in the Event of a Personal Data Breach

If becoming aware of a Personal Data Breach, the Processor shall notify the Controller in accordance with clause 7.6.

Such notification shall, as a minimum, contain the following information.

1. A description of the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
2. Communicate the name and contact details of the Processor’s data protection officer or other contact point where more information can be obtained;
3. A description of the likely consequences of the Personal Data Breach; and
4. A description of the measures taken or proposed to be taken by the Processor to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

On request the Processor shall assist the Controller in communicating a Personal Data Breach to the Data Subjects, taking into account the nature of processing and the information available to the Processor.

1. Impact Assessments and Advance Consultation

12.1 Where a type of Processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Processor shall, at its own cost, prior to the Processing, if necessary and upon request by the Controller, assist the Controller in an assessment of the impact of the envisaged Processing operations on the protection of Personal Data. A single assessment may address a set of similar Processing operations that present similar high risks.

12.2 If the assessment of the planned Processing shows that the Processing would, in lack of risk reducing measures from the Controller, lead to a high risk, the Processor shall assist the Controller in consultations with the supervisory authority, before commencing the Processing.

1. Transfer of Personal Data to a Third Country

13.1 The Processor is not entitled to transfer Personal Data to a third country or an international organisation without the Controller first providing its written consent to such transfer.

13.2 A transfer to a third country presupposes under every circumstance, i.e. also when the Controller has provided its written consent, that the Processor fulfils the requirements and implements the measures pursuant to the GDPR with regard to third country transfer.

1. Damage and Liability

14.1 In case of claims from Data Subjects for material or immaterial damage due to the Processing, GDPR Art 82 shall apply and paragraph 5 of Art 82 shall be employed for claim back of compensation corresponding to the other Party’s part of the responsibility for the damage. The Processor is at this liable also for damages caused by sub-processors engaged by the Processor.

14.2 For damages other than what follows from 14.1 of this Agreement, the Parties are liable in accordance with the service agreement (see Section 2 of this Agreement). The Parties acknowledge that administrative fines according to Art 83 of GDPR or coherent national legislation do not constitute damage in the sense of this Clause 14.2 and that such administrative fines shall encumber the Party that has been imposed by the administrative fine.

14.3 The Parties shall inform each other if they become aware of a circumstance that may result in damages or payment liability of the other Party and work together to prevent and minimize such damages or payment liability.

14.4 Before a Party engages in any negotiations, enter into any settlement or agreement or obligates itself to any other undertaking in relation to the Data Subjects or any other third party or a court of law or authority based on any claim or sanction under clauses 14.1-14.2, the Party shall give the other Party the opportunity to assist in the matter or otherwise exercise its rights.

1. Contact Persons

15.1 For notifications of Personal Data Breach, information on contact with the regulatory authorities or Data Subjects or other communication of importance for the Processing, the Processor shall first of all turn to the Data Protection Officer at the Controller:

dataskyddsombud@uu.se

15.2 Contact at the Processor for the Processing is:

[contact information]

1. Amendments and Modifications

16.1 Amendments and modifications to this Agreement shall be in writing and signed by authorised representatives of both Parties to be valid. However, the Controller may at any time modify the instructions set out in **Appendix 1** in accordance with Clause 5.1 of this Processor Agreement**.**

16.2 If the contents of the service change, such as by new functions being added or by new ways of processing Personal Data that may arise, the Controller shall immediately be notified in writing of the changes.

1. Termination

17.1 Upon termination of the Agreement, the Personal Data shall either be returned to the Controller or be deleted. Unless otherwise notified by the Controller, the Personal Data shall be returned to the Controller and then deleted at the Processor within 30 days if no other time limit is set out in the instructions in **Appendix 1**. Upon request, the Processor shall provide a written notice of which measures have been taken in relation to the Personal Data in connection with the Processing being terminated.

17.2 If the Processor due to law, ordinance, authority regulations or decisions is obliged to keep Personal Data after this Agreement has ceased to apply, such Personal Data may only be used for the purpose presented by the relevant law, ordinance, authority regulation or decision that gives rise to the Personal Data being kept. The Controller shall be informed of this and the reasons therefore.

1. Transfer of Agreement

The Processor is not entitled to transfer its obligations under this Agreement in part or in whole to another party without written consent from the Controller.

1. Agreement Period

This Agreement shall enter into force when both Parties have signed the agreement and be valid for as long as the Processor Processes Personal Data on behalf of the Controller.

1. Applicable Law and Disputes

20.1 The Parties’ rights and obligations under this Agreement is governed by Swedish law.

20.2 Disputes regarding the interpretation or application of this Agreement shall be decided in accordance with Swedish law and addressed in Swedish public court. If the Processor is a Swedish authority, disputes shall instead be ultimately decided by the immediately superior authority or otherwise by an available dispute resolution mechanism within the Swedish Government.

-------------------------------

[Signature page follows]

This Agreement has been prepared in two (2) identical original copies out of which the Parties have each received one (1).

**Uppsala University** [Processor’sname]

*Signature Signature*

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

*Place and date Place and date*

**Appendix 1**

**Controller’s instructions**

The Parties have specified below what is included in the Processing under the Agreement.

1. **Purpose of the Processing**

The purpose of the Processing of Personal Data is *(why is the Processing of Personal Data carried out, e.g. delivery of product under the Main Agreement, carry out xxxx, handle salary payments, etc.).*

1. **Categories of Data Subjects**

The categories of Data Subjects affected are *(which groups of residents are Processed in the system, e.g., municipal residents, pensioners, savers, pupils, employees in the unit, elected representatives, individuals receiving a service, people participating in product development, etc.).*

1. **What kind of Personal Data is Processed**

The Personal Data transferred is of the following type: *(e.g. name, IP address, e-mail address, property designation, sole proprietorship, etc.).*

1. **Sensitive/Integrity-sensitive Personal Data (where applicable)**

The sensitive Personal Data that the transfer comprises is *(e.g. race or ethnic origin, political views, religious or philosophical conviction, union membership, health and disease and Processing of genetic and biometric information. In the Processing of sensitive Personal Data, particular attention shall be paid to the handling being carried out in accordance with the Swedish Tax Agency’s guide for secrecy-marked Personal Data in public administration.).*

1. **Processing**

The Personal Data will be Processed in the following way *(compare clause 3 in the Data Agreement, such as collection, registration, organisation, storage, processing and distribution or other provisioning of information, compilation or joint processing. Please note that if sensitive Personal Data is Processed, it shall be listed here as “Processing of sensitive Personal Data”).*

1. **Processing in a Third Country (where applicable)**

*(State if Personal Data is transferred, directly or indirectly, to a country outside the EU/EEA.)*

1. **Termination routines**

See clause 17 in the Agreement. *(If a longer period than 30 days is needed for deletion of the Personal Data at the Processor, this must be stated here.)*

1. **Approved sub-processors**

*(State possible sub-processors below.)*

|  |  |  |
| --- | --- | --- |
| **Name of sub-processor** | **Type of Processing and purpose of the Processing** | **Location of Processing and, when the Processing is outside of the EU/EEA, the lawful basis for the transfer of Personal Data**  |
|  |  |  |
|  |  |  |

**Appendix 2**

**Information security measures in relation to the Processing**

[All processing of Personal Data must be protected by information security measures that ensure a relevant level of security based on the sensitivity of the information. If you have questions regarding the text in Appendix 2, please contact the Security and Safety Division, the Information Security Department.]

The Controller has carried out information classification and an analysis based on information security requirements according to Swedish and international standards SS-ISO / IEC 27001

**The Processor guarantees that**

* information security work is conducted in accordance with ISO/IEC 27001 or equivalent in this area
* development of the company's information systems/ IT services is carried out with regard to information security requirements of confidentiality, integrity and availability.
* access control, integrity, traceability and availability is fundamental in the Processor’s management of information security.
* premises are protected by locks and alarms. Documented p procedures are available for allocation and handling of equipment and permissions and are reviewed regularly
* administrative routines and technical measures are available in order to separate data from different customers
* follow-up of IT security incidents is carried out in accordance with the implemented management systems for information security
* all personal data incidents that concern the Client's data are reported to Uppsala University according to the contact information obtained
* IT environment and the IT services that the Processor uses for information management meet the below requirements.

**Basic requirements for the Processor´s IT environment and IT services**

The Processor must ensure that:

* protective mechanisms are available in the form of a firewall
* only authorised personnel have access to the Processor's IT environment
* the communication between: 1) web client and server and 2) machine to machine is protected with SSL/TLS (TLS, at least version 1.2)
* disc areas and separate files must be encrypted. Crypto-algorithms and key lengths recommended by NIST, SP 800-131 must be used for encryption.
* the life cycle of certificates and crypto keys must be documented
* requirements for passwords are met; consist of at least 10 characters, constitute a mixture of different characters
* access rights management is implemented to protect against unauthorized access to information
* all users' activities in the system are logged and the logs must be stored securely
* logs are protected against unauthorized change and unauthorized access
* the system supports multi-factor authentication
* databases must be encrypted.