

DATA PROCESSING AGREEMENT

Agreement in accordance with Article 28.3 of EU General Data Protection Regulation 2016/679¹

This Data Processing Agreement was reached (27/11/2019) by the parties below

Controller	Processor
Company reg. number	Company reg. number
Address	Address

1 BACKGROUND AND PURPOSE

1.1 This Data Processing Agreement is part of the master agreement on the provision of services entered into by the Swedish Arts Council (Kulturrådet) and the service provider and should be read and understood in this context. The Data Processing Agreement governs the Processor's processing of Personal Data on the Controller's behalf (hereafter referred to as (the) processing).

1.2 The purpose of this Data Processing Agreement is to safeguard the rights and freedoms of Data Subjects when the Swedish Arts Council engages a Processor for the Processing of Personal Data, and to ensure compliance with Article 28.3 of EU General Data Protection Regulation 2016/679, hereafter referred to as the Data Protection Regulation.

2 DEFINITIONS²

Personal data 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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by

¹ EU General Data Protection Regulation 2016/679 stipulates that a written agreement must be in place on the Processor's Processing of Personal Data on the Controller's behalf.

² See Article 4 of EU General Data Protection Regulation 2016/679

transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Protection Legislation	Any privacy or personal data legislation, or any other legislation (including regulations and provisions), which are applicable to the Personal Data Processing that will take place under this Agreement, including national legislation kind and EU Legislation, as may be amended over time.
Logging	The continuous collection of data regarding the processing, in accordance with the agreement, of personal data that may be associated with an individual physical person.
Controller	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.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Personal data	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.
Personal data breach	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.
Filing System	Any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.
Data subject	The person to whom the personal data relates.

Third Country

A state that is not a member of the European Union or a party to the European Economic Area.

3 PERSONAL DATA PROCESSING; PURPOSE AND TYPE OF PERSONAL DATA

3.1 The Processor may only process the Controller's personal data in accordance with this agreement and the related written instructions in order to carry out their work for the Controller.

4 The Controller's responsibilities

4.1 The Controller undertakes to ensure that there is a legal basis for the processing in question in accordance with paragraph 3 and to issue written instructions so that the Processor and any subprocessors are able to deliver their services in accordance with this Data Processing Agreement (Appendix 1).

4.2 The Controller shall own all of the data that the Processor collects for the purpose of meeting their obligations under the master agreement. The above shall apply even if the parties agreed otherwise before the Data Protection Regulation entered into force.

4.3 The Controller shall be responsible for informing **pre-existing** Data Subjects about the processing in accordance with the agreement, and, where necessary, for obtaining the consent of Data Subjects and defending their right to transparency and erasure, and so on.

4.4 The personal data that the Processor directly collects from Data Subjects, for the purpose of meeting their obligations under the master agreement, shall be owned by the Controller. The above shall apply regardless of anything previously agreed.

4.5 The Controller undertakes to provide information cards to the Processor so that the Processor can meet their obligations in accordance with 5.2.

5 THE PROCESSOR'S COMMITMENTS

5.1 The Processor undertakes to only process personal data for the purposes set out in Appendix 1 and to comply with the Data Protection Legislation or other relevant legislation relating to the Processing of Personal Data, and to stay informed about the applicable law in this area.

5.2 The Processor undertakes to provide Data Subjects with information about processing when personal data are collected. The information may be provided verbally through a reference to the Controller's official website or, if this is specifically requested by the Data Subject, through the providing of an information card. If the Data Subject is under the age of 18, the Processor should inform the person who has parental responsibility for the child by the same means.

5.3 The Processor must take measures to protect the personal data against any kind of unauthorised processing.

5.4 The Processor undertakes to ensure that all of the people working under their management comply with the contents of this Data Processing Agreement, and the currently applicable instructions from the Controller, and that they are informed of the relevant legislation.

5.5 At the Controller's request, the Processor shall assist them with impact assessments and prior consultations, and with producing information in connection with the Master Agreement in force.

5.6 If the Processor finds that some of the Controller's instructions, in accordance with Appendix 1, are unclear, unlawful or lacking, and the Processor judges them to be necessary to meet their commitments, they must promptly inform the Controller of this and await new instructions.

6 SECURITY MEASURES

6.1 The Processor undertakes to take all of the appropriate technical and organisational security measures in accordance with the Data Protection Legislation or other relevant legislation, and to take any measures stated in the instructions³ to protect the personal data.

6.2 In cases where the Processor processes sensitive personal data covered by a confidentiality obligation, the Controller may request additional security measures.

6.3 The Processor must have procedures and tools that prevent the unauthorised processing of, or unauthorised access to, personal data. The Processor must be able to trace the Processing of Personal Data through Logging. These logs must be covered by the necessary protection measures.

6.4 The Processor must be able, through an authorisation control system, to actively restrict access to personal data to persons who are working under their management and need the personal data to carry out their work tasks for the performance of the agreement between the Processor and the Controller.

6.5 The Processor undertakes to continuously log access to personal data in accordance with this agreement to the extent required in accordance with the instructions (Appendix 1). Logs may be weeded no sooner than five (5) years after Logging unless otherwise stated in the instructions.

7 CONFIDENTIALITY

7.1 The Processor, and the staff working under this Data Processing Agreement, must comply with document confidentiality and professional secrecy obligations when processing personal data. Personal data that are managed in connection with this agreement may not be

³ If, due to the master agreement, Data Subject to confidentiality rules is to be made technically accessible to a person who does not need to access the data in question, the agreement should be drafted in such a way that it is unlikely that the service provider, or any other unauthorised person, will actually access the data. In such a situation, the data should not be deemed to have been disclosed within the meaning of the Public Access to Information and Secrecy Act.

used or disseminated for other purposes, either directly or indirectly, unless this has been approved in writing by the Controller.

7.2. The Processor must ensure that all of the employees, consultants and other persons whom the Processor is responsible for, and who process personal data, are subject to a confidentiality undertaking. This is not required, however, if they are already covered by an obligation of professional secrecy established by law and subject to criminal penalties. The Processor also undertakes to ensure that confidentiality agreements are in place with any subprocessors, and that confidentiality undertakings have been signed between subprocessors and their staff.

7.3 The Processor must promptly notify the Controller of any contact with supervisory authorities regarding the Processing of Personal Data. The Processor does not have the right to represent the Controller, or act on the Controller's behalf, in dealings with supervisory authorities relating to such processing.

7.4 If Data Subjects, supervisory authorities or third parties request information from the Processor about the Processing of Personal Data, the Processor must inform the Controller. Information about the Processing of Personal Data may not be given to third parties without the written approval of the Controller. The Processor must assist with the relaying of information that is covered by an approval.

8 REVIEWING, OVERSIGHT AND AUDITING

8.1 At the Controller's request, the Processor must promptly provide all of the information concerning, for example, the technical and organisational security measures necessary for the Controller to be able to review and oversee the Processor's Processing of Personal Data as a result of this Data Processing Agreement.

8.2 The Processor undertakes to audit its Personal Data Processing security at least once a year through an internal audit to check that the Processor's Processing of Personal Data complies with this Data Processing Agreement. The result shall be reported to the Controller upon request.

8.3 The Controller has the right to monitor, themselves or through a third party designated by them (who must not be one of the Processor's competitors), the Processor's compliance with the Processing requirements imposed by the Controller. In the event of such monitoring, the Processor must assist the Controller, or whoever is carrying out the review, by providing the documentation, access to the premises and IT systems, and other access, that are necessary to monitor the Processor's compliance with this Data Processing Agreement.

8.4 The Processor has the right to offer alternative monitoring methods, however, such as a review by an independent third party. In such a case, the Controller shall have the right, but not the obligation, to adopt this alternative monitoring method. In the event of such an audit or check, the Processor must provide the Controller, or a third party, with the assistance needed for its conducting.

8.5 The Processor must provide the supervisory authority, or any other authority that is concerned with Personal Data Processing, or authority to whom it may be relevant, with the opportunity to carry out on-site supervision.

8.6 The Processor must also guarantee the same rights for the Controller in respect of any Subprocessors engaged.

9 RECTIFICATION AND ERASURE OF PERSONAL DATA and Operation and maintenance

9.1 The Processor undertakes to promptly rectify incorrect or incomplete personal data as instructed by the Controller. After the Controller has requested rectification that entails the deletion of personal data, the Processor may only process the personal data as part of the rectification process and undertakes to promptly take the necessary measures, within 30 days at the latest.

9.2 If the Processor is considering making changes in their systems (upgrades, troubleshooting, etc.) in a way that might be expected to affect information management, the Processor must consult the Controller about this. Such information must be provided well in advance of the change.

10 Personal data breaches

10.1 The Processor undertakes to assist the Controller with the meeting of their obligations in the event of a Personal Data Breach. The Processor must assist with the investigation of any suspicions that an unauthorised person has processed, or had unauthorised access to, personal data.

10.2 In the event of Personal Data Breaches, or the risk of such, the Processor must inform the Controller of the event promptly and in writing. The Processor must provide the Controller with a written description of the Personal Data Breach. This must include:

1. The nature of the Personal Data Breach and, where possible, the categories and number of Data Subjects affected, and the categories and number of personal data records affected,
2. The probable consequences of the Personal Data Breach, and
3. The measures that have been taken or suggested, and the measures to mitigate the Personal Data Breach's potential adverse effects.

11 SUBPROCESSORS

11.1. The Processor is obliged to inform the Controller when they engage new subprocessors. The Processor must in this case sign an agreement and ensure that the subprocessor is covered by the same conditions as apply to the Processor. The Processor shall bear full responsibility towards the Controller for any subprocessors engaged.

11.2 If the Processor is considering engaging subprocessors, they must provide information about the type of data and categories of Data Subjects a given subprocessor would deal with,

and their capacity and ability to meet their obligations in accordance with the Data Protection Legislation and other relevant legislation relating to the Processing of Personal Data.

11.3 The Processor must forward a copy of the agreement with the subprocessor at the Controller's request.

11.4 The Processor undertakes to also inform the Controller of any plans to stop working with an approved subprocessor.

12 TRANSFERRING OF PERSONAL DATA TO THIRD COUNTRIES AND LOCATION

12.1 The Processor must ensure that the personal data are (managed and) stored within the EU/EEA, unless otherwise agreed by the parties.

12.2 Paragraphs 12.3 and 12.4 shall apply if the Controller accepts data transfers to third countries. See Appendix 1.

12.3 The Processor only has the right to transfer personal data to third countries, for example for service, support, maintenance, development, operation or similar management, if the Controller has approved such transfers and issued specific instructions (Appendix 1).

12.4 Data may only be transferred to third countries if the Data Protection Legislation and other relevant legislation, and this agreement and the related instructions, are complied with.

13 LIABILITY FOR DAMAGE

13.1 The Processor undertakes to hold the Controller harmless against any material or non-material damage as a result of the Controller becoming liable to pay damages to a third party, in accordance with Article 82 of the Data Protection Regulation, if the Personal Data Processing that was the basis for the compensation for damages was carried out by the Processor or a subprocessor in violation of the Data Protection Legislation or other relevant legislation in the area, this Data Processing Agreement or instructions from the Controller.

13.2 The Processor undertakes to also otherwise hold the Controller harmless should the Controller suffer harm as a result of the Processor processing Personal Data in violation of this Data Processing Agreement.

13.3 If the Controller becomes aware of circumstances that might lead to liability for damages or payment obligations for the Processor, the Controller must immediately inform the Processor of the situation and actively work with the Processor to prevent and minimise such liability for damages or payment obligations.

14 JURISDICTION AND DISPUTE RESOLUTION

14.1 Swedish law shall be applicable to this agreement. Any differences in interpretation or disputes in connection with the agreement that the Parties cannot resolve themselves shall be settled by the Swedish civil courts.

15 ADDITIONS OR AMENDMENTS TO, OR THE TERMINATION OF, THE AGREEMENT

15.1 To be valid, any additions or amendments to this Data Processing Agreement must be made in writing and signed by both Parties.

15.2 The Parties have the right to request the renegotiation of this agreement and any appendices if

1. the ownership of the other party changes significantly, or
2. the applicable legislation or the interpretation of it changes in a way that affects the Personal Data Processing covered by this agreement, or
3. the engaging of subprocessors is not approved by the Controller.

15.3 A request for amendments from either party does not entail the breaking of the Data Processing Agreement, just the starting of renegotiation.

15.4 Each Party has the right to terminate the agreement in writing if the other party commits a significant breach of the provisions of this agreement, and fails to rectify the situation within thirty (30) days of receipt of a written request for such from the other Party.

A notice period of three (3) months shall apply upon the termination of the agreement.

15.5 If the Controller objects to any change of subprocessor, they shall have the right to terminate the service and receive a refund of the charges paid for the remaining period.

16 TERM OF THE AGREEMENT AND CEASING OF PROCESSING

16.1 This Data Processing Agreement shall apply until further notice, and cease to apply when the Processor has stopped processing Personal Data on the Controller's behalf. When the Data Processing Agreement ceases to apply, for whatever reason, all of the personal data must be transferred to the Controller, at the Controller's request, in an agreed standardised or open format, or deleted.

16.2 Personal data must be deleted on an ongoing basis unless otherwise agreed, and within 30 days at the latest. In the event of the transferring of personal data, the same term shall apply after the transfer has taken place. This also applies to other related information such as instructions, system solutions, descriptions or other documents that the Processor has received through exchanges of information in accordance with this Data Processing Agreement.

16.3 The Processor must also surrender the logs to the Controller in the agreed standardised or open format if this agreement ceases to apply.

16.4 The confidentiality provisions in paragraph 7 shall also continue to apply after this Data Processing Agreement has otherwise ceased to apply.

17 SUNDRY

17.1 The Parties shall each designate a contact person with responsibility for collaboration between the Parties. The other party must be notified in writing of any change of contact person or contact details.

17.2 The payment of remuneration in connection with this Data Processing Agreement, and any additional costs incurred by the Processor in order to meet their obligations in accordance with this agreement, shall be governed by the master agreement.

The Data Processing Agreement has been drafted in two (2) copies, which each of the Parties has received one of.

Authorised signatory for

The Controller
The Processor

Town/city and date

Signature

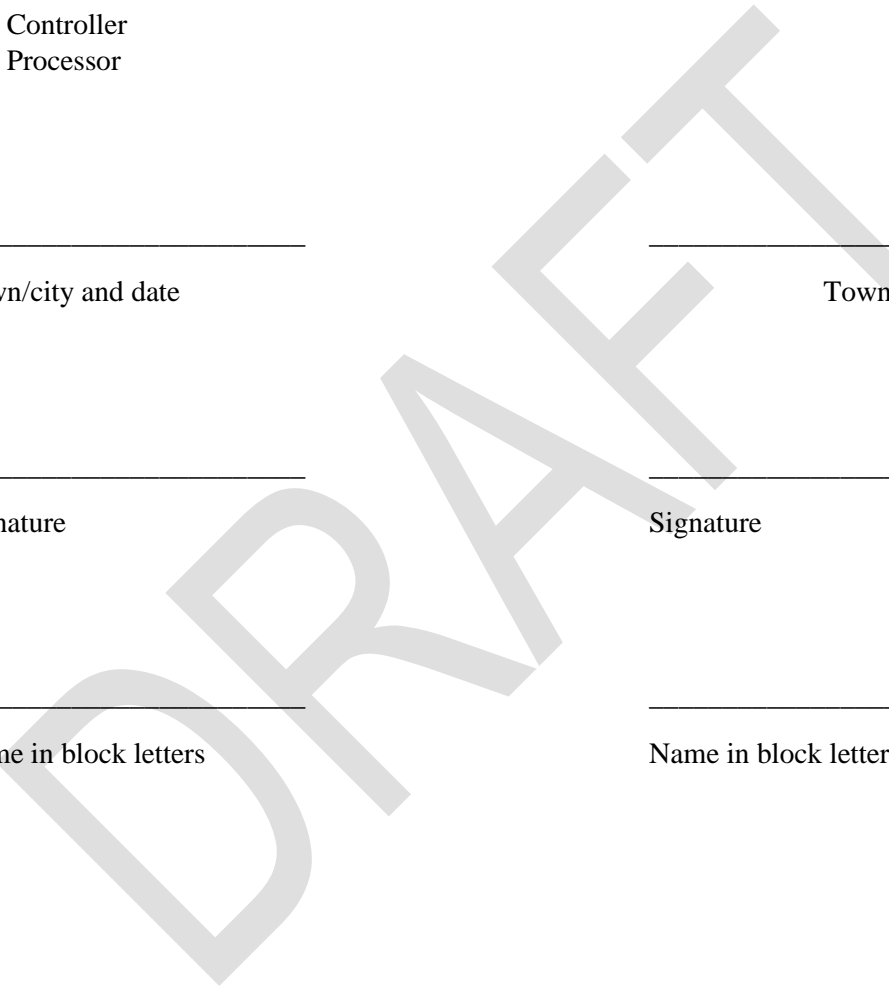
Name in block letters

Authorised signatory for

Town/city and date

Signature

Name in block letters



Appendix 1 – Personal data management instructions

In addition to what has already been stated in this agreement, the processor must also comply with the following instructions:

<p>Purpose Briefly describe the purpose of the personal data that the processor will process. Describe where the information will be stored.</p>	<p>Example: The Controller is processing personal data in order to carry out its government assignment and to comply with Swedish law.</p> <p>The Personal Data Processing is therefore necessary as</p> <ul style="list-style-type: none"> • the authority is carrying out an assignment that is in the public interest and is part of the exercise of public authority, and/or • the authority is fulfilling a legal obligation and/or • the authority is complying with an agreement. <p>Example: All of the personal data in the system for support, technical maintenance and back-up purposes. The information is to be stored in [Country]</p>
<p>The processing covers the following types of personal data State which personal data the processor will have access to.</p>	<p>Example: The personal data in the system consists of</p> <ul style="list-style-type: none"> • User names • Personal ID numbers • Xxx • Xxx <p>The processor is also responsible for transferring the following data to system Y through technical integration</p> <ul style="list-style-type: none"> • Xxx • Xxx • xxx
<p>The processing covers the following categories of Data Subjects State the categories of Data Subjects whose data the processor has access to or will process.</p>	<p>Example:</p> <ul style="list-style-type: none"> • Employees • Job seekers • Consultants • Patients • Students • Guardians

<p>State the specific management requirements for the Personal Data Processing to be carried out by the processor.</p> <p>Add clarifying descriptions if necessary, for example regarding data weeding</p>	<p>Example 1:</p> <ul style="list-style-type: none"> • Personal data must be weeded after x years • Backups must not be saved for more than x years • The processor may only publish information that contains first names on website x. <p>Example 2: See the master agreement, section x.x</p> <p>Example 3: The processor must refer Data Subjects to the Swedish Arts Council's official website when personal data is collected from them. The reference may be verbal. If a Data Subject requests this, the Processor must provide an information card.</p>
<p>State the specific technical protection measures for the Personal Data Processing carried out by the processor.</p> <p>Add clarifying descriptions if necessary.</p>	<p>Example 1: The service provider must meet the requirements stated based on the Controller's information classification and report the status on request.</p> <p>Example 2: See the master agreement, section x.x</p>
<p>State the specific Logging requirements for the Personal Data Processing and who will have access to the data.</p>	<p>Example: Logs must state: The history of changes in a grade for individual students and who made the changes</p> <p>Example 2: No specific requirements beyond what is stated in the master agreement.</p>
<p>Transferring of personal data to third countries</p>	<p>Example 1: Only personal data about staff, students and guardians related to support cases in the form of contact details (names, telephone numbers and email addresses) may be transferred to the Processor's subprocessor (see Appendix B2).</p> <p>Example 2: The following personal data may be transferred to third countries: Users' shoe sizes Users' first names</p>
<p>Other instructions regarding the personal data management carried out by the processor</p>	<p>Example 1: Setting up of remote access to the Controller's system to investigate and address technical problems; and Publication of pseudonymised statistics on the number of applications made in the system and the expected waiting time for processing for the website indicated.</p> <p>Example 2:</p>

	<p>Paragraph 7.3 of the Data Processing Agreement does not apply to this service.</p> <p>Example 3: Paragraph 16.3 of the Data Processing Agreement has been amended as follows.</p> <p><i>16.3 The Processor shall also surrender the logs to the Controller only in XML format if this agreement ceases to apply.</i></p>
--	---

DRAFT

Appendix B2 List of subprocessors

The countries where the respective companies are established and from which staff may process data are stated in brackets.

Processing of support cases, conversations and other support requests from the Controller.

- E.g. Processor Limited (UK)
- E.g. Processor (Ireland)
- (E.g. Processor Corporation (USA))

Setting up of remote access to the Controller's system to investigate and address technical problems.

- Outside companies (subprocessors):
- E.g. subprocessor ABC AB (Sweden)
- E.g. subprocessor CDE AB (Sweden)

DRAFT