

# PERSONAL DATA PROCESSOR AGREEMENT

Agreement in accordance with Article 28.3 of the General Data Protection Regulation EU 2016/679<sup>1</sup>

This Personal Data Processor Agreement is concluded (00.00.2018) between:

# (referred to below as the “Personal Data Controller”), organisation registration number #, based at address # and, # (referred to below as the “Personal Data Processor”), organisation registration number #, based at address # (jointly referred to as the “Parties”) have this day entered into the following Personal Data Processor Agreement.

## 1 BACKGROUND AND PURPOSE

1.1 This Personal Data Processor Agreement is part of a main agreement on the provision of services, which has been concluded between the Municipality/County Council/Region and the supplier, and shall be read and understood against this background. The Personal Data Processor Agreement regulates the processing of Personal Data by the Personal Data Processor on behalf of the Personal Data Controller and the level of privacy that shall be attained during the Processing (referred to below as (the) processing).

1.2 The purpose of this Personal Data Processor Agreement is to ensure the registered persons’ freedoms and rights when the Municipality/County Council/Region appoints a Personal Data Processor for the processing of personal data, and to comply with Article 28.3 of the General Data Protection Regulation EU 2016/679, referred to below as the Data Protection Regulation.

## 2 DEFINITIONS<sup>2</sup>

Processing of personal data	Measures or combination of measures in respect of personal data or sets of personal data, regardless of whether they are carried out in an automated manner or not, such as collection, registration, organisation, structuring, storage, processing or modification, development, reading, using, disclosure through transfer, dissemination or provision by other means, adjustment or amalgamation, limitation, deletion or destruction.
Data Protection Act	Refers to such privacy and personal data legislation and any other legislation (including regulations and directives) that applies to the personal data processing that is carried out under this Agreement, including such national legislation and EU legislation as may be amended over time.

<sup>1</sup> The General Data Protection Regulation EU 2016/679 stipulates that there must be a written agreement on the processing of personal data by the Personal Data Processor on behalf of the Personal Data Controller.

<sup>2</sup> In accordance with Article 4 of the General Data Protection Regulation EU 2016/679

Personal data controller	Natural or legal person, public authority, institution or other body that determines, alone or together, the purposes and the means of the processing of personal data.
Personal data processor	Natural or legal person, public authority, institution or other body that processes personal data on behalf of the personal data controller.
Personal data	Any piece of information that relates to an identified or identifiable natural person (registered person), whereby an identifiable natural person is a person who can be identified directly or indirectly as distinct by reference to an identifier such as a name, an identification number, a localisation detail or online identifier, or one or more factors that are specific to the natural person's physical, physiological, genetic, mental, economic, cultural or social identity.
Personal data incident	A security incident that leads to unintentional or unlawful destruction, loss or modification, or to unauthorised disclosure of or unauthorised access to the personal data that are transferred, stored or otherwise processed.
Register	A structured collection of personal data that is accessible in accordance with specific criteria, regardless of whether the collection is centralised, decentralised or dispersed on the basis of functional or geographical conditions.
Registered person	The person the personal data relates to.
Third country	A state that is not included in the European Union or associated with the European Economic Area.

### 3 THE PROCESSING OF PERSONAL DATA, THE PURPOSE, TYPE OF PERSONAL DATA

3.1 The purpose of the processing of the personal data (*insert a description of the purpose and where the information can be found*). The Personal Data Processor may only process the Personal Data Controller's personal data for the purpose stated in the agreement and the Personal Data Controller's written instructions for fulfilling his duties towards the Personal Data Controller, for example, but not limited to,

- health and patient care,
- social service,
- pre-school, primary and secondary education,
- community building,
- development and the economy,
- public transport,
- culture,

- personal and financial administration, and
- control of persons and addresses

#### **4 RESPONSIBILITIES OF THE PERSONAL DATA CONTROLLER**

4.1 The Personal Data Controller undertakes to ensure that there is a legal basis for the current processing in accordance with Clause 3 and to draw up written instructions to enable the Personal Data Processor and any subcontracting processors to carry out their duties in accordance with the personal data processor agreement (appendix 1).

4.2 The Personal Data Controller undertakes to inform the Personal Data Processor without delay of changes in the processing that affect the obligations of the Personal Data Processor pursuant to current Data Protection Act or other relevant legislation.

4.3 The Personal Data Controller is responsible for advising registered persons of the processing carried out in accordance with the agreement and, if required, for obtaining the registered person's consent, and for safeguarding the right of registered persons to data transparency, deletion, etc.

#### **5 OBLIGATIONS OF THE PERSONAL DATA PROCESSOR**

5.1 The Personal Data Processor undertakes to process the personal data only for the purposes stated in Clause 3 of this agreement and to observe the applicable Data Protection Act or other relevant legislation in respect of the processing of personal data, and to keep informed of applicable laws in the area.

5.2 The Personal Data Processor shall take measures to protect the Personal Data against destruction, modification, unpermitted dissemination and unauthorised access and also against other forms of unpermitted processing.

5.3 The Personal Data Processor undertakes to ensure that all persons working under his leadership comply with the stipulations of this Personal Data Processor Agreement and the instructions that may be given by the Personal Data Controller at any time, and also to be informed of the relevant legislation.

5.4 The Personal Data Processor shall assist the Personal Data Controller as necessary in providing information that is requested by a third party.

5.5 If the Personal Data Processor finds that the Personal Data Controller's instructions, as stated in Appendix 1, are unclear, unlawful or missing, and the Personal Data Processor believes these are necessary for him to meet his obligations, the latter shall inform the Personal Data Controller of this without delay and await new instructions.

#### **6 SECURITY MEASURES**

6.1 The Personal Data Processor is obliged to take all suitable technical and organisational security measures in accordance with applicable data protection legislation and any measures stipulated in the instructions<sup>3</sup> in order to protect the personal data.

---

<sup>3</sup> If the service agreement implies that information regulated by secrecy is to be made technically available to a party that does not need to have sight of the information in question, the agreement should be worded in such a way that it is unlikely that the service provider or any other unauthorised person will actually have sight of the information. In such a situation, the information should not be regarded as disclosed in the sense of the law on public access to personal data and the Secrecy Act.

6.2 If the Personal Data Processor processes sensitive personal data that are subject to confidentiality, particularly high requirements for security are set. The Personal Data Controller may then give further instructions for security measures.

6.3 The Personal Data Processor shall have an authorisation control system that impedes the unauthorised processing of personal data or unauthorised access to personal data. The Personal Data Processor shall use a logging system that makes it possible for the processing of personal data to be traced, and shall also ensure that the logs have adequate security protection.

6.4 The Personal Data Processor shall use the authorisation control system to actively prevent access to the personal data of such persons who work under his management and who need the personal data in order to carry out their work duties for the fulfilment of the agreement between the Personal Data Processor and Personal Data Controller.

## **7 CONFIDENTIALITY**

7.1 The Personal Data Processor and the personnel working under this Personal Data Processor Agreement shall respect their duty of confidentiality when processing personal data. The personal data, information, instructions, system solutions, descriptions or other documents that the Personal Data Processor receives through the exchange of information in accordance with this Personal Data Processor Agreement or other agreement between the parties may not be used or disclosed for any other purpose than that stipulated in this Personal Data Processor Agreement or other agreement between the parties, whether directly or indirectly, if the Personal Data Controller has not consented to this in writing.

7.2 The Personal Data Processor undertakes to ensure that all employees, consultants and other persons for whom the Personal Data Processor is responsible and who process the personal data are bound by a confidentiality clause. (Confidentiality clauses are not required if the Personal Data Processor and his personnel are bound by a duty of confidentiality sanctioned by penalties in accordance with the law.) The Personal Data Processor also undertakes to ensure that there are appropriate confidentiality agreements in place with any Subcontracting Processor and a confidentiality clause governing the relationship between the Subcontracting Processor and his personnel.

7.3 The Personal Data Processor shall inform the Personal Data Controller in writing without delay of any contacts with a supervisory authority that concern or may be of significance for the Processing of the Personal Data. The Personal Data Processor does not have the right to represent the Personal Data Controller or act on behalf of the Personal Data Controller in dealings with supervisory authorities on matters that concern or may be of significance for the Processing of the Personal Data.

7.4 If Registered Persons, supervisory authorities and other third parties request information from the Personal Data Processor concerning the Processing of Personal Data, the Personal Data Processor shall refer these persons to the Personal Data Controller. The Personal Data Processor may not disclose Personal Data or other information on the Processing of Personal Data without the prior written permission of the Personal Data Controller. The Personal Data Processor undertakes, on receiving such permission, to assist in providing registered persons, supervisory authorities or other third parties with information on the processing of personal data.

## **8 INSPECTION, SUPERVISION AND AUDITING**

8.1 At the request of the Personal Data Controller, the Personal Data Processor shall provide, without delay, all information, e.g. technical and organisational security measures that the Personal Data Controller needs to be able to inspect and exercise his right to transparency in the Personal Data Processor's processing of personal data, as provided for by this Personal Data Processor Agreement.

8.2 The Personal Data Processor undertakes to conduct an annual audit of the security of the personal data processing by means of an internal audit in order to check that the processing of personal data by the Personal Data Processor complies with this Personal Data Processor Agreement. The Personal Data Controller must be advised of the result.

8.3 The Personal Data Controller has the right to monitor, or to appoint a third party (who must not be a competitor of the Personal Data Processor) to monitor the Personal Data Processor's compliance with the Personal Data Controller's requirements for the Processing. In the event of such monitoring, the Personal Data Processor shall assist the Personal Data Controller or the person carrying out the inspection with documentation, access to premises, IT systems and other access that is required to enable monitoring of the Personal Data Processor's compliance with this Personal Data Processor Agreement.

8.4 The Personal Data Processor has the right, however, to propose an alternative approach to the monitoring, for example, an inspection carried out by an independent third party. The Personal Data Processor shall in such case have the right, but not be obliged to, apply this alternative approach to the monitoring. In the event of such auditing or checking, the Personal Data Processor shall give the Personal Data Controller or a third party the assistance that is needed for its implementation.

8.5 The Personal Data Processor shall give a supervisory authority, or other authority that concerns or may be of significance for the Processing of Personal Data the opportunity to view on site.

8.6 The Personal Data Processor shall also assure the Personal Data Controller similar rights in respect of hired Subcontractor Processors.

## **9 CORRECTION AND DELETION OF PERSONAL DATA AND OPERATION AND MAINTENANCE**

9.1 The Personal Data Processor undertakes to make corrections (correct, delete or block) of erroneous or incomplete personal data without delay in accordance with the Personal Data Controller's instructions.

After the Personal Data Controller has requested a correction of personal data in writing, the Personal Data Processor may only process the personal data as part of the correction process and undertakes to complete the action without delay, but within 90 days at the latest.

9.2 Before the Personal Data Processor and his subcontracted processors put their systems into operation for the receipt or provision of data in accordance with this agreement, the systems shall undergo quality assurance through testing in a test environment.

9.3 The Personal Data Processor undertakes to continuously log access to personal data in accordance with this agreement in the extent required for the instructions (Appendix 1). Logs may not be deleted until after five (5) years of the time of logging.

9.4 If the Personal Data Processor intends to make modifications to his systems (upgrades, troubleshooting, etc.) in a way that can be expected to affect the processing of information, the Personal Data Processor shall consult the Personal Data Controller about this. Such information shall be provided in good time before the modification.

## **10 PERSONAL DATA INCIDENTS**

10.1 The Personal Data Processor shall provide and implement technical and practical solutions to investigate suspicions that an unauthorised person has processed or gained unauthorised access to the Personal Data. In the event of unauthorised Processing, unauthorised access, destruction or modification of Personal Data, as well as attempts at these, the Personal Data Processor shall inform the Personal Data Controller of the incident in writing immediately.

10.2 The Personal Data Processor undertakes to assist the Personal Data Controller to meet the latter's obligations under Article 32 of the Data Protection Regulation. According to Article 33 of the Data Protection Regulation, personal data incidents, intrusion attempts or other fraudulent activity to gain access to the Personal Data Controller's personal data shall be reported to the Personal Data Controller's contact person by the Personal Data Processor without delay.

10.3 The Personal Data Processor shall provide the Personal Data Controller with a description of the personal data incident. This shall

1. give an account of the type of the personal data incident and, if possible, the categories and number of registered persons affected, and also the categories and number of personal data items affected.
2. give an account of the likely consequences of the personal data incident, and
3. give an account of the actions that have been taken or proposed, as well as the measures to mitigate the potential negative effects of the personal data incident.

## **11 SUBCONTRACTOR PROCESSORS**

11.1 The Personal Data Controller has the right to object to the hiring of Subcontractor Processors other than those stated in Appendix 2. The Personal Data Processor does not have the right to hire Subcontractor Processors for the processing of personal data without the Personal Data Controller's written approval.

11.2 If the Personal Data Processor intends to hire Subcontractor Processors, the latter shall provide information on what type of data and categories of registered persons a Subcontractor Processor is to deal with, and the latter's capacity and ability to fulfil his obligations in accordance with the Data Protection Act and other relevant legislation in respect of the processing of personal data.

11.3 After approval, the Personal Data Processor may sign an agreement with Subcontractor Processors. According to such agreement, the Subcontractor Processors shall become bound by similar conditions for the processing of personal data to those stipulated in this Personal Data Processor Agreement. The Personal Data Processor shall send a copy of the agreement with the subcontractor processor at the request of the Personal Data Controller.

11.4 The Personal Data Processor also undertakes to inform the Personal Data Controller of any plans to stop using an approved subcontractor processor.

## **12 TRANSFER OF PERSONAL DATA TO A THIRD COUNTRY AND LOCALISATION**

12.1 The Personal Data Processor may only transfer personal data to third countries, for example, service, support, maintenance, development, operation or similar processing, if the Personal Data Controller has approved such transfer in writing and issued separate instructions (Appendix 1).

12.2 Before transfer is begun, the Personal Data Processor shall provide documentation confirming that the requirements of the current Data Protection Act or other relevant legislation and the instructions to this Personal Data Processor Agreement are met.

12.3 The Personal Data Processor shall ensure that the personal data are stored within Sweden/the EU, unless the parties have agreed otherwise in writing.

### **13 LIABILITY FOR DAMAGE**

13.1 The Personal Data Processor is obliged to indemnify the Personal Data Controller for material or immaterial damage in the event that the Personal Data Controller becomes liable to pay damages to anyone pursuant to Article 82 of the Data Protection Regulation, if the Processing of Personal Data on which the compensation for damages is based has been carried out by the Personal Data Processor or a subcontractor processor in

contravention of the Data Protection Regulation, this Personal Data Processor Agreement or instructions from the Personal Data Controller.

13.2 The Personal Data Processor is also obliged to otherwise indemnify the Personal Data Controller in the event that the Personal Data Controller incurs damage as a consequence of the Processor's processing of Personal Data in contravention of this Personal Data Processor Agreement.

### **14 LAW AND DISPUTE RESOLUTION**

14.1 Swedish law shall apply to this agreement. Any interpretation or dispute in respect of the agreement that the parties are unable to resolve themselves shall be settled in an ordinary Swedish court.

### **15 SUPPLEMENTS, AMENDMENTS OR TERMINATION OF THE AGREEMENT**

15.1 Supplements and amendments to this Personal Data Processor Agreement shall not be valid unless they are made in writing and signed by both Parties.

15.2 The Parties have the right to invoke a renegotiation of this agreement and other appendices in the event of

1. an essential change to the counter-party's ownership, or
2. if the applicable legislation or interpretation thereof changes in a way that affects the processing of personal data covered by this agreement.

15.3 A request for a change by either party does not imply that the Personal Data Processor Agreement is suspended, only that a renegotiation is initiated.

### **16 PERIOD OF AGREEMENT AND TERMINATION OF PROCESSING**

16.1 This Personal Data Processor Agreement is valid indefinitely and only terminates when the Personal Data Processor has concluded the processing of Personal Data on behalf of the Personal Data Controller. When the Personal Data Processor Agreement is terminated, for whatever reason, all Personal Data shall be returned to the Personal Data Controller in a format specified by him.

16.2 The Processor undertakes to delete all Personal Data that are processed in accordance with this Personal Data Processor Agreement within 180 days of termination. The Data shall not be deleted,

however, before the Personal Data Processor has advised the Personal Data Controller in writing when the deletion is to take place and has returned the Personal Data.

This also applies to other associated information such as instructions, system solutions, descriptions or other documents that the Personal Data Processor has received through the exchange of information in accordance with this Personal Data Processor Agreement.

16.3 The Personal Data Processor shall also provide the Personal Data Controller with the logs in the agreed format if this agreement ceases to be valid.

16.4 The provisions on confidentiality in Clause 7 shall continue to be valid even after this Personal Data Processor Agreement has otherwise ceased to be valid.

16.5 Either Party has the right to terminate the agreement in writing. If the agreement is terminated, a notice period of three (3) months shall apply.

A Party is entitled to terminate this agreement if the counter-party;

1. is guilty of an essential breach of a provision of this agreement and fails to rectify the breach within thirty (30) days of receipt of a written request from the other Party to do so, or
2. is made bankrupt, initiates composition negotiations or is otherwise insolvent.

16.6 If the Personal Data Controller objects to a replacement of a subcontractor processor, the latter has the right to terminate the service and receive reimbursement for the fees paid for the remaining period.

## 17 OTHER

17.1 The Parties shall each appoint a contact person with responsibility for the Parties' cooperation. The other party shall be informed in writing of a change of contact person or contact details.

17.2 Compensation due under this Personal Data Processor Agreement and any additional costs the Personal Data Processor incurs in order to fulfil his obligations under this agreement are regulated by the main agreement.

This Processor Agreement has been drawn up in two (2) copies, one of which has been given to each Party.

Authorized signatory for  
Personal Data Controller

Authorized signatory for  
Personal Data Processor

\_\_\_\_\_  
Place and date

\_\_\_\_\_  
Place and date



Signature:

---

Name in clear script

Signature:

---

Name in clear script

## Appendix 1 - Instruction for processing of Personal Data

In addition to what is already stipulated in this agreement, the Personal Data Processor shall also follow the instructions given below:

### Personal Data Processing

<p><b>Purposes</b></p> <p>Specify all purposes for which the Personal Data Processor will be processing personal data.</p>	<p>(insert a description of all purposes and where the data can be found). The Personal Data Processor will be processing personal data for the purpose of providing services in accordance with the Service Agreement.</p>
<p><b>Categories of personal data</b></p> <p>Specify categories of personal data that will be processed by the Personal Data Processor.</p>	<p>Insert, e.g.;</p> <p>The following categories may be included in the processing of personal data.</p> <ol style="list-style-type: none"> <li>1) Personal data concerning the Personal Data Controller's personnel, mainly contact details; <ul style="list-style-type: none"> <li>Name,</li> <li>Position</li> </ul> </li> <li>2) Personal data concerning the Personal Data Controller's patients, including health-related and potentially sensitive information; and <ul style="list-style-type: none"> <li>Personal identity numbers</li> <li>Sickness absence/absence</li> <li>Patient details</li> <li>Data relating to personal circumstances (social services)</li> <li>Testimonials</li> </ul> </li> </ol>
<p><b>Categories of registered persons</b></p> <p>Specify all categories of registered persons whose details will be processed by the Personal Data Processor.</p>	<p>Insert, e.g.;</p> <p>The categories of registered persons include the Personal Data Controller's:</p> <ol style="list-style-type: none"> <li>1. Personnel; <ul style="list-style-type: none"> <li>Employees</li> <li>Job seekers</li> <li>Consultants</li> <li>Users of the IT system (AD login)</li> </ul> </li> <li>2. Individual persons; <ul style="list-style-type: none"> <li>Patients</li> <li>Clients</li> <li>Pupils</li> <li>Close family relatives/parents</li> </ul> </li> </ol>

<p><b>Special security requirements</b></p>	<p>Insert, e.g.;</p> <p>The Personal Data Processor and any subcontractor processor shall undertake technical, administrative and organisational measures to ensure a level of security that is appropriate for the risk, including;</p> <ol style="list-style-type: none"> <li>1. pseudonymisation and encryption of personal data,</li> <li>2. the ability to continuously ensure the confidentiality, privacy, accessibility and resistance of the information system and e-services,</li> <li>3. the ability to restore accessibility and access to personal data within a reasonable timescale in the event of a physical or technical incident, and</li> <li>4. a procedure for regularly testing, examining and evaluating the efficiency of the technical and organisational measures that are to ensure the security of the processing.</li> </ol>
<p><b>Logs</b></p>	<p>Insert, e.g.;</p> <p>The Personal Data Processor and Subcontractor Processor shall be responsible for ensuring that</p> <ol style="list-style-type: none"> <li>1. the access documentation (logs) states what measures have been carried out in respect of data concerning a registered person,</li> <li>2. the logs specify for which unit the measures have been taken,</li> <li>3. the logs specify at what time the measures have been taken,</li> <li>4. the logs specify the identity of the user and the registered person,</li> <li>5 systematic and recurrent spot checks of the logs are carried out, and</li> <li>6. checks of the logs are documented.</li> </ol>
<p><b>Transfer of personal data to a third country</b></p> <p>The extent to which personal data may be transferred outside the EEA for the purpose of providing the services in accordance with the Service Agreement.</p>	<p>Insert, e.g.;</p> <p>As part of the Personal Data Processor's implementation of the services provided under the Service Agreement, <i>anonymised</i> personal data relating to support cases and personal data in the form of contact details such as the name, telephone number and e-mail address of the Personal Data Controller's personnel may be transferred to the Personal Data Processor's subcontractor processor, see Appendix 2.</p> <p>(Any subcontractor processors in the USA must be connected to Privacy Shield.)</p>
<p><b>Purging time</b></p> <p>Specify the purging time for when the personal data processed by the Personal Data Processor are to be purged.</p>	<p>Insert, e.g.;</p> <p>The Personal Data Controller shall determine the purging times (number of years) for personal data.</p>
<p><b>Practical processing</b></p> <p>Specify how the processing is to be carried out.</p>	<p>Insert, e.g.;</p> <p>Personal data may be processed by the Personal Data Processor if this is required for the provision of the services in accordance with the Service Agreement.</p> <p>This may include, from time to time, for example:</p>

	<ol style="list-style-type: none"><li>1) Establishing remote access to the Personal Data Controller's system in order to investigate and remedy technical problems; and</li><li>2) Processing support cases, conversations and other support enquiries from the Personal Data Controller.</li></ol>
--	---

## Appendix 2 List of subcontractor processors

The countries in which respective companies are established and from which personnel may process personal data are given in brackets.

Processing support cases, conversations and other support enquiries from the Personal Data Controller.

E.g. Personal Data Processor Limited (United Kingdom)

E.g. Personal Data Processor (Ireland)

E.g. Personal Data Processor Corporation (USA)

Establishing remote access to the Personal Data Controller's system in order to investigate and remedy technical problems.

External companies (subcontractor processors):

E.g. the ABC AB subcontractor processor (Sweden)

E.g. the CDE AB subcontractor processor (Sweden)