

Data Processor Agreement

Configura Sverige AB

Company registration no.: 556404-7156

Box 306

SE-581 02 Linköping, Sverige

("Data Processor")

Company registration no.:

("Data Controller")

and

(individually called a "party" and collectively "the parties ")

Has entered this Agreement

on the Data Processor's processing of personal data on behalf of the Data Controller

1. The processed personal data

- 1.1 This Agreement has been concluded in connection with the parties' conclusion of an agreement to develop and maintain software for 2D and 3D drawings of Data Controllers Solutions and Products, and related services.
- 1.2 The Data Processor processes the types of personal data as set out in Appendix 1, on behalf of the Data Controller. The personal data relates to the registered persons listed in Appendix 1.
- 1.3 The Data Controller is entitled to delete and/or add additional types of personal data and/or registered persons to the above list by sending a new list of personal data and / or registered persons to the Data Processor.

2. Purpose

- 2.1 The Data Processor may only process personal data for purposes that are necessary to test new and existing functionality as well as correct malfunction of the software in connection herewith.

3. The Data Processors obligations

- 3.1 The Data Processor may only process the personal data transferred by the Data Controller in accordance with the Data Controllers instructions and is also obliged to comply with the personal data law currently in force.

The Data Processor must take the necessary technical and organizational security measures, including additional measures that might be necessary preventing that the personal data listed in paragraph 1.2 accidentally or illegally are destroyed, lost or deteriorated and preventing that the personal data is known to unauthorized persons, exploited or is processed in violation of the Personal Data Legislation. The Data Processor is thus obliged to

- introduce log-in and password procedures and set up and maintain a firewall and anti-virus software;
- ensure that only employees with employment related purposes have access to the personal data;
- ensure that the employees involved in processing personal data have committed themselves to confidentiality or are subject to statutory professional secrecy;
- store data storage media properly so that they are not available to third parties;
- ensure that buildings and systems used for data processing are safe and that only high-quality hardware and software are being used, which is continuously being updated;
- ensure that samples and waste material are destroyed in accordance with the requirements for data protection complying further instructions from the Data Controller. In special cases, as determined by the Data Controller, said samples and waste material must be stored or returned;
- ensure that employees receive appropriate training, adequate instructions and guidelines for processing personal data. The Data Processor is committed to ensuring that the employees involved in the processing of personal data are familiar with the safety requirements.

- 3.2 If the Data Processor processes personal data in another EU/EEA member country, the Data Processor must comply with the legislation on security measures in that member country.

- 3.3 The Data Processor is required to immediately inform the Data Controller of operational malfunctions, suspected breach of data protection rules or other irregularities relating to the processing of personal data. In case of security breach, the Data Processor must notify the Data Controller immediately and no later than 72 hours after the security breach has been discovered. The Data Processor must, at the request of the Data Controller, assist the Data Controller regarding the security breach, including any notification to the Data Protection Authority and/or registered persons.
- 3.4 At the Data Controllers request, the Data Processor must provide the Data Controller with sufficient information to ensure that the Data Processor has taken the necessary technical and organizational security measures.
- 3.5 If the Data Processor or another data processor who has received information, receives a request for access to registered personal data from a registered or his/her agent, or a registrant objects to the processing of his/hers registered personal data, the Data Processor must immediately send such request and/or objection to the Data Controller for further process by the Data Controller unless the Data Processor is entitled to handle such inquiries himself/herself. The Data Processor must at the request of the Data Controller assist the Data Controller in relation to answering the request and/or the objection.

4. Transfer of information to other Data Processors or third parties

- 4.1 The Data Processor is solely obliged to transfer personal data mentioned in section 1.2 to other data processors or third party if the Data Controller provides written instruction about this. The Data Processor is not entitled to pass on or hand over personal data to third parties or other data processors without prior written instruction from the Data Controller unless such passing or handing over follows the legislation.
- 4.2 Before transferring personal data to another data processor (sub data processor) the Data Processor must ensure that the sub data processor has entered a written Data Processor Agreement stating that the sub data processor is accepting to be entering back-to-back terms relating to the conditions in this Agreement.
- 4.3 If the personal data is transferred to foreign sub data processors, the Data Processing Agreement must state, that it is the Data Protection Legislation of the Data Controller which applies to the foreign sub data processors. If the receiving sub data processor is established within the EU, the Data Processing Agreement must state that compliance with the specific regulatory requirements of data processing countries such as requirements for notification to national authorities, must be met by the receiving EU country. The Data Processing Agreement must be submitted to the Data Controller prior to the transfer of personal data to ensure it meets the terms of this Agreement.
- 4.4 The Data Processor must enter into written Data Processing Agreements with sub data processors within the EU/EEA in their own name. Regarding sub data processors

outside EU/EEA the Data Processor must enter standard agreements in accordance with the Commission's decision 2010/87/EU of February 5, 2010 concerning standard contract regulations of transmission of personal data to data processors established in 3rd countries under the terms of the European Parliament and Councils directive 95/46/EF (" Standard Agreement").

- 4.5 The Data Controller hereby grants the Data Processor the power of attorney to enter into standard agreements with sup data processors within the EU/EEA on behalf of the Data Controllers name provided that the Data Controller prior has given written instructions in accordance with paragraph 4.1.

5. Change

- 5.1 In case of changes in the Data Protection Legislation in the country where the Data controller entity is registered the Data Controller is entitled to change the instructions in this Agreement with 4 (four) weeks written notice upon transmission of new written instructions to the Data Processor, so that the Data Processor at all times comply with the current Personal Data Legislation.

6. Entry into force and termination

- 6.1 The Agreement enters into force on [insert date].
- 6.2 The parties can terminate this Agreement with 3 (three) months written notice terminating by end of month. The Agreement however cannot be terminated by the Data Processor the first 6 (six) months from date of entry. The Data Processor is however bounded by this Agreement if the Data Processor handles personal data on behalf of the Data Controller.
- 6.3 In the event of termination of the Agreement the Data Controller is entitled to demand that the personal information is returned to the Data Controller on media selected by the Data Controller or demand the personal information to be deleted.

7. Applicable law and jurisdiction

- 7.1 This Agreement is governed by Swedish law.
- 7.2 Any claim or dispute originating from or otherwise is connected to this Agreement must be settled by at the same venue as "CSAB Service Agreement" and "CSAB Collaboration Agreement".

8. Signatures

- 8.1 This Agreement is signed in two identical original copies of which each Party receives a copy.

On behalf of the Data Controller

On behalf of the Data Processor

Name:
Date & Place

Name:
Date & Place:

Appendix 1 - Types of personal data

<u>Data type</u>	<u>Detailed explanation</u>
Consumer identification number	
Consumer name	
Consumer address	Street name, Zip, City, Country/State
Consumer e-mail	
Consumer telephone number	
Consumer offer details description	Items, prices, volume, date, id number,
Consumer order details description	Items, prices, volume, date, id number,
System user (license taker) name	
System user (license taker) address	Street name, Zip, City, Country/State
System user (license taker) e-mail	
System user (license taker) telephone number	
System user (license taker) Company	
System user (license taker) sales representative	