DATA PROCESSING AGREEMENT

This **Data Processing Agreement**, the ("**Agreement**"), is made by and between TSHK, (the "**Processor**"), and the Client, (the "**Controller**").

The Processor and the Controller are individually referred to as "**Party**" and jointly as "**Parties**".

BACKGROUND

(A) This Agreement is part of the Processor's Terms and Conditions which form part of an agreement for the provision of services entered into between the Processor and the Controller (the "**Service Agreement**"). Under the Service Agreement the Processor will process Data on behalf of the Controller when supplying the services under the Service Agreement.

(B) The Controller is the data controller in relation to the processing of the Data. The Processor is a data processor, processing the Data on behalf of the Controller. Service Agreements which contain processing of Data on behalf of the Controller are specified in Appendix 1 under "Categories of Data".

1 DOCUMENTS

This Agreement consists of this main document and the following appendices:

Appendix 1: Instructions to the Processor

Appendix 2: Security Measures

Appendix 3: Approved Sub-Processors

2 DEFINITIONS AND INTERPRETATION

In this Agreement, capitalised terms shall have the meanings set out below or if not defined herein, the meanings set forth in Applicable Legislation.

Applicable Legislation means the GDPR and applicable supplementary legislation to the GDPR.

Data means the personal data (as defined in Applicable Legislation), specified in Appendix 1 hereto.

GDPR means Regulation (EU) 2016/679 of the European Parliament and the Council as amended, supplemented and/or varied from time to time.

Service Agreement means as set forth under Section "(A) Background" above in this Agreement.

3 INSTRUCTIONS

3.1 The Processor shall process the Data in accordance with the Controller's written instructions set forth in Appendix 1. The instructions shall at least include the following information:

(i) The purpose of the processing;

(ii) The character of the processing;

(iii) The duration of the processing, or how the duration will be decided;

(iv) Categories of personal data included in the Data; and

(v) Categories of data subjects included in the processing.

3.2 The Processor may not process the Data for any other purposes or in any other way than as instructed by the Controller from time to time. The Parties shall update Appendix 1 in the event of new or amended instructions. The Processor is entitled to charge any work carried out by it to comply with any new or amended instructions from the Controller on a time and material basis in accordance with the price agreed on between the Parties or its standard consultancy rates.

3.3 Notwithstanding the above, the Processor may undertake reasonable day-to-day actions with the Data without having received specific written instructions from the Controller, provided that the Processor acts for and within the scope of the purposes stated in Appendix 1.

3.4 In the event that the Processor considers that an instruction violates Applicable Legislation, the Processor shall refrain from acting on such instruction and shall promptly notify the Controller and await amended instructions.

4 THE CONTROLLER'S OBLIGATION TO PROCESS DATA LAWFULLY

4.1 The Controller shall ensure that a legal ground recognized under Applicable Legislation applies for processing of the Data. The Controller shall further meet all other obligations of a data controller under Applicable Legislation (including requirements to properly inform the data subjects of the processing of the Data).

4.2 The Controller's instructions to the Processor for the processing of the Data shall comply with Applicable Legislation. The Controller is responsible for the accuracy of the Data and for the lawfulness of the processing and acquisition of the Data.

5 SECURITY MEASURES

5.1 The Processor shall maintain adequate security measures to ensure that the Data is protected against destruction, modification and proliferation. The Processor shall further ensure that the Data is protected against unauthorized access and that access events are logged and traceable. The security measures are further described in Appendix 2. The Controller agrees that these security measures are adequate, sufficient and appropriate.

5.2 The Processor shall ensure (i) that only authorized persons have access to the Data, (ii) that the authorized persons process the Data only in accordance with this Agreement and the Controller's instructions and (iii) that each authorized person is bound by a confidentiality undertaking to the Processor in relation to the Data.

5.3 In the event of a personal data breach involving the Data, the Processor shall notify the Controller promptly after becoming aware of it. Furthermore, the Processor shall assist the Controller in ensuring compliance with the Controller's obligations to (i) document any personal data breach, (ii) notify the applicable supervisory authority of any personal data breach and (iii) communicate such personal data breach to the data subjects, in accordance with Applicable Legislation.

6 THE PROCESSOR'S OBLIGATIONS TO ASSIST

6.1 The Processor shall, taking into account the nature of the processing, assist the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests from data subjects for exercising their rights in Chapter III of the GDPR. The data subjects' rights include (i) rights to object to the processing and have the Data erased, (ii) rights to request information about and access to the Data, (iii) if technically viable, rights to move Data from one controller to another, and (iv) rights to request correction of Data.

6.2 The Processor shall, taking into account the nature of processing and the information available to the Processor, further assist the Controller in ensuring compliance with its obligations under Articles 32-36 of the GDPR. Such obligations include (i) to ensure security of the processing, (ii) to make data protection impact assessments and (iii) to make prior consultations with the supervisory authority.

7 SUB-PROCESSORS

7.1 The Processor may engage third parties to process Data on its behalf ("**Sub-Processor**"), if the Processor has informed the Controller thereof in writing and the Controller has not objected in writing within ten days after the Processor provided such information to the Controller. In such event the Sub-Processor becomes approved by the Controller ("**Approved Sub-Processor**"). Approved Sub-Processors are listed in Appendix 3 hereto (which shall be updated in the event of changes to the Approved Sub-Processors). Appendix 3 shall list the following information regarding each Approved Sub-Processor:

(i) name, contact information, company form and geographical location,

(ii) a description of the services provided,

(iii) the location of the Data that the Approved Sub-Processor processes.

7.2 The Processor shall enter into a written agreement with every Sub-Processor, in which the Sub-Processor undertakes obligations at least reflecting those undertaken by the Processor under this Agreement.

7.3 In the event the Controller objects to a Sub-Processor becoming an Approved Sub-Processor in accordance with in Section 7.1 above, then the Processor shall refrain from using such Sub-Processor for processing the Data. The Processor shall in such event use reasonable efforts to make a reasonable change in the services to the Controller to avoid that the Sub-Processor at hand processes the Data. In the event the Processor finds that such change is not practically or commercially reasonable the Processor shall be entitled to terminate the Agreement on 45 days' notice. The Processor must provide notification of termination to the Controller within 45 days from the day the Controller notified the Processor of its objection to the new Sub-Processor.

7.4 When the Controller has approved a Sub-Processor, the Controller is not entitled to object to such Sub-Processor.

8 TRANSFERS TO THIRD COUNTRIES

The Processor may not transfer Data outside of the EU/EEA without the Controller's written consent. In addition, such transfer may only be carried out if at least one of the following prerequisites is fulfilled:

(i) the receiving country has an adequate level of protection of Data as decided by the European Commission,

(ii) the Controller confirms that the data subject has given his/her consent to the transfer,

(iii) the transfer is subject to the European Commission's standard contractual clauses for transfer of personal data to third countries,

(iv) the Processor is subject to Binding Corporate Rules to which the receiving party in the third country is also subject, or

(v) for transfers to the United States, the receiving legal entity is certified under the EU-U.S. Privacy Shield.

9 AUDIT

9.1 Upon the Controller's request, the Processor will provide to the Controller information that demonstrates the Processor's compliance with its obligations under Applicable Legislation.

9.2 The Controller shall be entitled on 20 days' written notice to carry out an audit of the Processor's processing of the Data and information relevant in that respect to demonstrate that the Processor complies with this Agreement and Applicable Legislation. The Processor shall assist the Controller and disclose any information necessary in order for the Controller to carry out such audit. The Controller shall carry the costs for such audit.

9.3 If a Data Protection Authority carries out an audit of the Processor which may involve the processing of the Data, the Processor shall promptly notify the Controller thereof.

10 REMUNERATION

10.1 The Processor is remunerated for its processing of the Data as part of the fees for the services under the Service Agreement.

10.2 The Controller shall compensate the Processor for additional costs for any altered or additional instructions provided to the Processor regarding the processing or handling of the Data. Such compensation shall be on a time and material basis in accordance with the Processor's at each time applicable fees for consultancy services.

11 LIABILITY AND LIMITATION OF LIABILITY

The Processor's liability under this Agreement is subject to the provisions on limitation of liability in the Service Agreement.

12 CONFIDENTIALITY

12.1 The Processor undertakes not to disclose or provide any Data, or information related to the Data, to any third party. For the avoidance of doubt, an approved Sub-Processor shall not be considered a third party for the purposes of this Section 12.

12.2 Notwithstanding Section 12.1 above, the Processor may disclose such information if the Processor is obliged hereto by law, judgement by court or by decision by a competent authority. When such obligation arises, the Processor shall promptly notify the Controller in writing before disclosure, unless restricted from doing so under Applicable Legislation.

12.3 The confidentiality obligation will continue to apply also after the termination of this Agreement without limitation in time.

12.4 Furthermore, the Processor shall observe confidentiality in regard of the Data as stated under section 13 in the Processor's Terms and Conditions.

13 RETURN AND DELETION OF DATA

13.1 The Controller shall upon termination of the Service Agreement instruct the Processor in writing whether or not to transfer the Data to the Controller.

13.2 The Processor will in any event erase Data from its systems no earlier than 30 days and no later than 40 days after the effective date of termination of the Service Agreement. The Processor shall upon the Controller's request confirm in writing that such erasure is fulfilled.

14 TERM

For any Service Agreement entered into prior to 25 May 2018, this Agreement shall enter into effect on 25 May 2018. In all other cases this Agreement shall enter into force the day the Service Agreement including the Terms and Conditions enter into force.

Irrespective of the term of the Service Agreement, this Agreement shall enter into force when the Processor starts processing the Data and shall terminate on the later date of when the Processor has erased the Data or ceased to process the Data in accordance with Section 13 above.

APPENDIX 1 – INSTRUCTIONS

Any processing carried out by the Processor shall be carried out in accordance with the following instructions. If the Processor processes Data in violation with these instructions, the Processor will be deemed data controller.

	INSTRUCTION
Purposes of the processing	To provide services as specified in the Service Agreement.
The character of the processing	The Processor will process the Data on behalf of the Controller to be able to provide services under the Service Agreement. For some of the services named below, the Data may contain sensitive data, e.g. for payroll services. Furthermore, the Data may contain personal identification numbers. As regards the respective services in particular, please note the Categories of Data below.
The period of the processing	Processing will continue during the term of the Service Agreement.
Categories of data subjects	Depending on the Service Agreement's character and scope, the Processor may process Data of categories of registered persons as follows: The Controller's employees, the Controller's representatives (such as board members; managing directors and authorized signatories), the Controller's contact persons.
Categories of Data	Categories of Data processed when fulfilling the Service Agreement **may** in regard of the relevant service consist of the following: **<u>All services:</u>** Name, e-mail address, telephone number
	<u>Payment of the Client's invoices (Bookkeeping department):</u> As above. <u>Payroll services:</u> Title, nationality, gender, date of birth, age, personal number, other national identification number (e.g. CPR, social security number, tax registration number or number of passport), home address, personal e-mail address, bank account and credit card information, sickness, absence (holiday, parental leave etc.), time

	INSTRUCTION
	registration, payroll and HR documentation. **<u>Services regarding virtual office:</u>** Title, nationality, gender, date of birth, age, personal number, other national identification number, home address, personal e-mail address, bank account and credit card information.
Any other instructions	N/A

APPENDIX 2 – SECURITY MEASURES

Technical and organisational security measures

The Processor is responsible for the technical and organisational security measures in the Processor's system. The Processor works constantly on data protection issues with regard to programs, services and processes.

This means that the Processor sees to that an appropriate level of security of e.g. encryption, access management, etc. exists. The Processor has a concept for erasing data and meets other requirements in terms of data protection and privacy.

Access to premises

The Processor processes Data in its own premises. Access to the premises is managed by a person-bound chip system which allows different access rights. The premises are secured by an alarm system. Only permitted personnel have access to stored Data and/or servers. Visitors are received by the reception and do not have access to the departments where the Data is being processed. The premises are fire protected.

Access to data systems

Any rights are solely administrated by the Processor's IT-support. All data systems are protected by password and the requirements on the safety-level are regulated in an internal policy. Only personnel involved in the matter have access with individual restrictive access rights.

Storage and back-ups

The Processor has own servers at its premises. The storage of back-ups takes place at two separate places in Stockholm with full redundancy and back-up is made on a daily basis. Only authorized personnel have physical access to the servers. The servers and the Processor's network are protected by firewall and anti-virus-software.

Protection of knowledge and information

The Processor's personnel is informed about data protection and privacy and bound by confidentiality agreements to prevent spreading of data, information and the Processor's clients' and users' Data. Only authorized personnel have access to information and the authorization is managed by the Processor's IT-support. Furthermore, external service providers, such as cleaning personnel, are carefully selected and bound by confidentiality agreements.

Security-related incidents

In case of a security-related incident which affects or may affect the Controller, the Processor immediately takes appropriate measures and informs the Controller's contact person.

APPENDIX 3 – APPROVED SUB-PROCESSORS

The Processor engages the following authorised sub-processors for services in the respective departments as below:

Department Payroll Services:

Flexapplications Sverige AB, Drottninggatan 22, 702 10 Örebro, Sweden

Org.-no. 556616-1948

Description of service: Registration of time and travel expenses for payroll

The Data is processed in Sweden.

Fortnox AB, Box 427, 351 06 Växjö, Sweden

Org.-no. 556469-6291

Description of service: Payroll-system

The Data is processed in Sweden.

Department Bookkeeping:

Fortnox AB, Box 427, 351 06 Växjö, Sweden

Org.-no. 556469-6291

Description of service: Bookkeeping system

The Data is processed in Sweden.