PERSONAL DATA PROCESSOR AGREEMENT

PARTIES

This personal data processor agreement ('Processor Agreement') has been entered into between:

Buyer/Client/Customer ('Controller'), and

The company within the Hogia Group that entered into the Service Agreement (see definition below) with Controller ('Processor'),

referred to separately as 'Party' and jointly as 'Parties'.

General

Processor is the company within the Hogia Group that is responsible for all Processor commitments towards the users of Hogia's standardized products and services.

This Processor Agreement is [used/signed] when Processor (i) operates a software on behalf of Controller, (ii) Controller uses any of Processor's standardized internet-based software services or (iii) Processor in any other way processes Controller's Personal Data, for example via remote access and other support related assignments (jointly "Services"). Controller has together with Processor signed a separate agreement which controls the use of Hogia-products and Hogia-services ("Service agreement").

When the Customer in his/her role as processor, uses the Services towards its customers ("End customer"), the End customer shall be the Controller and Hogia acts as Sub-processor towards the Customer. What follows this Processor Agreement concerning Hogia's role as processor shall also apply to Hogia's role as Sub-processor.

1. Definitions

Unless otherwise stated, terms shall have the same meanings as in the Applicable Data Protection Regulations, which among other things means that:

Processing means any operation or set of operations which is performed on personal data or on sets of personal data, 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.

Applicable Data Protection Regulations refers, until 24 May 2018, to Council Directive 95/46/EC, implemented in Swedish law through the Personal Data Act (PDA, 1998:204) and the Personal Data Ordinance (1998:1191). As of 25 May 2018, it refers to the General Data Protection Regulation (GDPR), (EU) 2016/679.

Sensitive personal data is defined in Section 13 of the Swedish PDA and, as of 25 May 2018, in Article 9 of the GDPR.

Personal data means any information relating to an identified or identifiable natural person (hereinafter '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 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, see Personal data above.

Third country means a country outside the European Economic Area ('EEA').

Sub-processor means a processor that is engaged by the Processor who is a party to this Processor Agreement and who Processes Personal Data on behalf of the Controller.

2. Personal data processing

2.1. The Processor shall only process Personal Data in accordance with this Processor Agreement, Applicable Data Protection Regulations and the Controller's from time to time applicable instructions; see Appendix 1.

2.2. Categories of registered and types of Personal Data given in Appendix 1, may be altered in conjunction with for example updates or change of the Services. All changes of instructions are informed via the Processor's customer information web ("Hogia Kundtorg") unless otherwise stated in this Processor Agreement. In events where the Controller does not have access to the Hogia Kundtorg, information concerning changed instructions is sent out via email or via other accepted way, in accordance with other communication with the Controller.

2.3. If it comes to the Processors attention that the Processing of Personal data violates the current Data protection regulations, the Processor shall as soon as possible inform the Controller.

2.4. The Processor may not process Personal Data for their own or any other purposes than those for which the Processor has been engaged by the Controller.

2.5. The Processor may not transfer Personal Data to a Third Country unless this is permitted in accordance with the contents of Appendix 1.

2.6. The Processor shall without unreasonable delay, and at most within thirty (30) days of the Controller's request, provide the Controller with access to the Personal Data that the Processor possesses and implement a requested alteration, erasure, restriction or transfer of these Personal Data. If the Controller has erased, or instructed the Processor to erase, the latter shall take such measures as necessary to prevent restoration of the Personal Data. The Processor is entitled to compensation in accordance with the applicable price list for any work done under this paragraph.

2.7. The processor does not have the ability to delete single Personal Data processed by the Processor on behalf of the Controller. However, the Controller can always delete any of its own Personal Data.

2.8. The Processor is obligated to maintain a record of the Processing that takes place on behalf of the Controller. Upon request, a copy of this record shall be provided to the Controller or the competent supervisory authority in a readable format. The record shall contain the following:

a) The name and contact details of the Processor and its data protection officer, if such an officer exists, as well as of the Controller on behalf of which the Processing is conducted. Where applicable, the contact details of any Sub-processors as well;

b) The categories of Processing that have been conducted on behalf of the Controller;

c) In applicable cases, transfers of Personal Data to a Third Country, information about which Third Country this concerns and which appropriate safeguards have been implemented; and

d) A general description of the technical and organisational security measures taken to achieve an appropriate level of protection.

3. Responsibilities of the controller

3.1. The Controller is responsible for the Processing of Personal Data being legal and taking place in accordance with the Applicable Data Protection Regulations, which includes providing information of the Processing to the Data subject and ensure that the Personal Data processed is correct.

3.2. The Controller shall immediately provide the Processor with correct information in the event of the instructions being incorrect, incomplete or otherwise in need of amendment.

3.3. The Controller shall only provide the Processor with access to the personal data that is necessary with consideration for the purpose of the Processing.

4. Capacity, capability and audit

4.1. The Processor guarantees that it has the necessary technical and organisational capacity and capability to fulfil its obligations under this Processor Agreement and the Applicable Data Protection Regulations.

4.2. The Processor shall at the request of the Controller, or an independent third party engaged by the Controller, demonstrate that the obligations stipulated in this section of the Processor Agreement and the Applicable Data Protection Regulations are fulfilled by without delay providing the Controller with relevant information and to a reasonable extent enabling and contributing to audits and inspections. Unless otherwise agreed the Processer is entitled to compensation for its work.

4.3. An audit in accordance with the preceding paragraph shall be conducted in such a way as not to imply a security- or integrity risk.

4.4. In case an audit according to above shows defect in the Processor's fulfilment of the Processor Agreement the Processor shall compensate the Controller with reasonable costs for the audit conducted and in case the Processor does not make a correction within thirty (30) days from the Controller's notice of the defect the Controller is entitled to immediately terminate the Service Agreement based on the relevant defect.

5. Security measures

5.1. The Processor shall via appropriate technical and organisational measures restrict access to the Personal Data and only provide authorisation to personnel who require access to the Personal Data in order to fulfil their commitments under this Processor Agreement, as well as to ensure that such personnel have the necessary training and have received sufficient instruction in how to handle the Personal Data in an appropriate and secure manner.

5.2. The Processor shall protect the Personal Data from all types of unauthorised Processing, such as destruction, unauthorised distribution and unauthorised access.

5.3. The Processor shall Process the Personal Data in confidence and ensure that persons authorised to Process the Data at the Processor have signed special non-disclosure agreements or have been informed that a special obligation of secrecy applies in accordance with contractual obligations or the applicable law.

5.4. Where the Processor Processes Sensitive Personal Data or otherwise processes Personal Data of a sensitive nature, that is covered by secrecy, there are particularly strict requirements.

5.5. Security measures taken are based on the information given in Appendix 1. In case the Controller intend to change the instructions by adjusting which categories of Personal Data to be processed by the Processor, and these changes results in increased requirements for security measures, the Controller shall with undue delay and in writing inform the Processor so that he/she is given the opportunity to adjust the security measures to the extent possible.

5.6. In case the Processor is unable to provide additional security measures within the scope of its activities the Controller is entitled to terminate the Service Agreement with a notice period of thirty (30) days.

5.7. The Processor shall without unreasonable delay, and at the latest within twenty-four (24) hours of the matter coming to the Processor's attention, notify the Controller about the occurrence or risk of a Personal Data Breach. Such notification shall include all necessary and available information that the Controller requires in order to take appropriate preventative measures and countermeasures, as well as to fulfil its obligations as regards notifying the competent supervisory authority of Personal Data Breaches.

6. Cooperation

6.1. The Processor shall, with consideration for the nature of the Processing, with appropriate technical and organisational measures help the Controller, to the extent this is possible, to fulfil its obligation to respond to requests to exercise the Data Subject's rights. Unless otherwise stipulated the Processor is entitled to compensation for such work.

6.2. The Processor shall assist the Controller in ensuring that the obligations concerning security associated with the Processing, Personal Data Breaches and impact assessments pursuant to the Applicable Data Protection Regulations are fulfilled, with consideration for the type of Processing and the information to which the Processor has access. Unless otherwise stipulated the Processor is entitled to compensation for such work. The security of the service covered by the Service Agreement is defined in a separate product description.

6.3. The Processor shall without unreasonable delay inform the Controller if the Processor has been contacted by the competent supervisory authority or another third party in order to gain access to the Personal Data that the Processor, or in applicable cases Sub-processor, has in its possession. The Processor shall only give a third party or supervisory authority access to the Personal Data processed if required by law.

6.4. The Processor shall in writing and in advance inform the Controller of planned changes to processing operations, including technical and organisational changes, that can affect the protection of the Personal Data and the Processor's compliance with the Applicable Data Protection Regulations. Before such changes are implemented, the Controller shall provide its consent, which shall not be unreasonably denied. In case the change negatively affects the Controller's ability to comply with applicable data protection rules, the Controller is entitled to terminate the Service Agreement with immediate effect.

7. Sub-processor

7.1. The Controller can of its own accord provide general written approval for the Processor to engage a Sub-processor for a certain type of personal data processing offered by the Processor to its customers. Existing Sub-processors are stated in Appendix 1. If such general approval has been provided, the Processor shall inform the Controller of its intentions to use or replace a Sub-processor in good time so that the Controller has the opportunity to raise objections to such a change. Such objections entail an obstacle to the Processor for implementing the proposed changes. I If the Processor engage a new Sub-processor or replace the existing Sub-processor despite such objection the Controller is entitled to terminate the Service Agreement given a notice period of thirty (30) days.

7.2. Such transfer of processing activities to a Sub-processor is conducted at the risk of the Processor and entails no changes to the division of responsibility that applies between the Parties to this Processor Agreement.

7.3. It is the responsibility of the Processor to with appropriate measures ensure that an engaged Sub-processor fulfils all applicable stipulations on the protection of Personal Data and in all essentials fulfils the obligations regulated by this Processor Agreement. It is the Processor's responsibility to ensure that an audit or inspection of the Sub-processor can be conducted by the Controller or the Processor in accordance with paragraph 4.2 above.

7.4. The Processor is entitled to fulfil all or part of the Service Agreement from other countries within the EU/EES by itself or by Sub-processors.

7.5. In case there is an integration between a Processor's and a, by the Controller engaged, third party Sub-processor's software such third party software shall not be considered as Sub-processor to Hogia. It is the Controller's responsibility, if required, to sign a service-/product agreement and, if required, a processor agreement with such third part.

8. Transfer to third country

8.1. In cases where the Processor in conjunction with the Processing transfers Personal Data to a Third Country which by the European Commission is not considered to provide an adequate level of protection in relation to the Applicable Data Protection Regulations, the Parties shall enter into an additional agreement governing this.

8.2. If the Processor has engaged a Sub-processor with the result that Personal Data are transferred to a Third Country which by the European Commission is not considered to provide an adequate level of protection in relation to the Applicable Data Protection Regulations, the Processor and the Sub-processor shall enter into an additional agreement. Where applicable, the Processor shall provide the Controller with a signed copy of such an additional agreement as that specified above.

9. Liability for damages

9.1. If a Data Subject has filed a claim for damages against the Controller or if a competent authority has issued a fine or other administrative penalty and this has been caused by the Processor Processing Personal Data in breach of the Controller's instructions, this Processor Agreement or the Applicable Data Protection Regulations, the Processor shall indemnify and hold the Controller harmless.

9.2. If a Data Subject has filed a claim for damages against the Processor or if a competent authority has issued a fine or other administrative penalty due to the Controller Processing Personal Data in breach of this Processor Agreement or the Applicable Data Protection Regulations, the Controller shall indemnify and hold the Processor harmless.

9.3. In the event that a Party is suffering from damages as a result of the other Party's processing of Personal Data in breach of this Processor Agreement or the Applicable Data Protection Regulations, both parties commits to hold each other harmless.

9.4. Each Party's liability towards the other Party for damages is limited to the amount equal to one (1) year fee for the software or service on which the claim is based.

10. Term

10.1. This Processor Agreement is valid from May 1st 2018 (or the later date when the Processor's processing of the Controller's Personal Data commence, i.e. when the Service Agreement is concluded) until the Processor's Processing of the Personal Data ceases or until it is replaced by a new processor agreement.

10.2. The Processor shall upon the termination of Processing return any Personal Data that the Processor has in its possession in a commonly used and readable format to the Controller (whenever possible, otherwise it is the responsibility of the Controller to extract the personal data before processing is terminated) and thereafter delete the Personal Data from such systems that have been used in the Processing, unless this conflicts with any mandatory legislation or if otherwise agreed by the Parties. The Processor is entitled to compensation for any return in accordance to this paragraph.

11. Conflict of law and dispute resolution

11.1. This Processor Agreement is subject to Swedish law, without taking into account its conflict-of-law rules.

11.2. Disputes arising from this Processor Agreement shall ultimately be resolved by arbitration according to the Stockholm Chamber of Commerce Arbitration Institute's Rules for Simplified Arbitration. The arbitration procedure shall take place in Gothenburg.
