Data Processing Agreement

Version 1.0 – 1 November 2017 -

DATA PROCESSING AGREEMENT

[XXXX]
[Address]
[Postal code and city]
Company reg. no.: [XXXX]
(hereinafter referred to as the "Data Controller")

and

CompuSoft A/S
Sunekær 9 5471
DK-Søndersø
Denmark
Company reg. no.:
(hereinafter referred to as the "Data Processor")

have entered into the following data processing agreement (hereinafter referred to as the "Data Processing Agreement" or the "Agreement")

relating to

[project or system name/title]

where data is stored

at CompuSoft's sites on Funen.

1 Background, Purpose and Scope.

1.1 As part of the Data Controller's entry into an agreement for the provision of services from CompuSoft A/S, the Data Processor undertakes to engage in the processing of personal data for which the Data Controller is responsible.

1.2 The Data Processor must comply with the Danish Act on Processing of Personal Data (Act No. 421 of 31 May 2000, with subsequent amendments) and its associated regulations.

1.3 As from 25 May 2018, the Data Processor shall instead comply with the General Data Protection Regulation (Regulation EU 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) with its related legal instruments as well as national legislation derived therefrom (rather than the Danish Act on Processing of Personal Data)

1.4 It is a requirement in both the Danish Act on Processing of Personal Data as well as the General Data Protection Regulation that a written agreement is entered into between the Data Controller and the Data Processor concerning the processing to be undertaken; what is referred to as a "data processing agreement." This Agreement constitutes such a data processing agreement.

1.5 The Data Processor may act only upon receiving instructions from the Data Controller. The Data Processor is required to take the requisite technical and organisational security measures so that information is not accidentally or unlawfully destroyed, lost or impaired, and to prevent that the unauthorised persons gain knowledge of the information, or that it is misused or otherwise processed in violation of the Danish Act on Processing of Personal Data. Upon the Data Controller's request, the Data Processor shall provide the Data Controller with sufficient information in order to ensure that the above-mentioned technical and organisational measures concerning security have been taken.

1.6 This Agreement is a supplement to "CompuSoft, Terms and Conditions for Hosting," which is to be considered as the "Hosting Agreement." These Terms and Conditions can be found at: **http://www.compusoft.dk/uploads/file/terms/Hosting-vilkår%201.pdf**.

2 Personal information encompassed within the Agreement

2.1 This Agreement and its accompanying instructions encompass all of the following types of personal data:

2.2 Name, address, telephone number, date of birth, usage history, payment information, residence history, family relationships, civil personal registration number, Internet usage and come-and-go statistics.

2.3 It is the responsibility of the Data Controller to ensure that data is provided to the Data Processor only after the end customer/guest has given their consent for the usage of personal data.

3 Geographical requirements

3.1 The processing of personal data that the Data Processor engages in pursuant to the agreement with the Data Controller may only be performed by the Data Processor, or Subcontracted Data Processor (see Section 5), within the European Economic Area (EEA). The Data Processor is not entitled. under any circumstances. to allow data processing to occur outside of the EEA without first receiving the Data Controller's written consent.

4 Instructions

4.1 The scope of the tasks that the Data Controller is to provide and support means that, according to the agreement between the Parties, there will be various different forms of processing of personal data. The different types of processing of personal data are described in Section 2.

4.2 The Data Processor may act only after receiving documented instructions from the Data Controller. The Data Processor must ensure that the personal data provided is not used for purposes, or otherwise processed, other than what is stated in the Data Controller's instructions. All the necessary and described acts of processing are considered to be documented in the Hosting Agreement.

a) If in the Data Processor's opinion an instruction is contrary to the Danish Act on Processing of Personal Data or the General Data Protection Regulation, the Data Processor shall inform the Data Controller accordingly.

b) This Agreement and its accompanying instructions primarily concern the Data Controller's customers/guests and employees.

c) If the processing of personal data by the Data Processor occurs in whole or in part via the usage of a remote connection, including home workplaces, the Data Processor shall establish guidelines for its employees' processing of personal data using remote connection, which must also comply with the requirements as set out in the Agreement.

d) The Data Processor shall, to the extent feasible, assist the Data Controller in fulfilling the Data Controller's obligations to respond to requests relating to the exercise of the rights of the data subjects, including transparency, rectification, limitation or deletion if the relevant personal data is processed by the Data Processor. If the Data Processor receives such inquiries from the data subject, the Data Processor will inform the Data Controller accordingly.

4.3 The Data Controller is responsible for all data processing costs associated with such assistance (see Section 4.6), including to the Subcontracted Data Processor. The amount to be paid for the Data Processor's assistance is to be determined in accord with the Data Processor's prevailing schedule of hourly rates for such work.

5 Use of Subcontracted Data Processors

5.1 The Data Controller gives the Data Processor permission to use Subcontracted Data Processors, provided that the terms and conditions of this Agreement are complied with. The Data Processor is to inform the Data Controller of such Subcontracted Data Processors.

5.2 The Subcontracted Data Processor acts under the Data Controller's instructions. The Data Processor has entered into a written data processing agreement with the Subcontracted Data Processor, which ensures that the Subcontracted Data Processor fulfils requirements similar to those imposed on the Data Processor by the Data Controller pursuant to the Agreement.

5.3 Any costs incurred in establishing the contractual relationship with a Subcontracted Data Processor, including the costs of establishing a data-processing agreement and the possible establishment of the basis for transfer to third countries, is to be borne by the Data Processor and thus the Data Controller has no responsibility for this.

5.4 If the Data Controller desires to instruct a Subcontracted Data Processor directly, this should only be done after consultation with and via the Data Processor. If the Data Controller issues instructions directly to the Subcontracted Data Processor, the Data Controller shall notify the Data Processor at the same time of the instructions and the background thereof. Where the Data Controller instructs a Subcontracted Data Processor directly, a) the Data Processor is released from any liability, and any consequences of such instructions is solely the Data Controller's responsibility, b) the Data Controller is responsible for any costs that the instructions may cause the Data Processor to incur, including that the Data Processor is entitled to invoice the Data Controller at its customary hourly rate for all working hours that such direct instructions may cause to the Data Processor; and (c) the Data Controller is itself liable vis-à-vis the Data Processors for any and all costs, remuneration or other payment to the Subcontracted Data Processor, which the direct instruction may cause to arise.

5.5 The Data Processor uses individual Subcontracted Data Processors.

5.6 At the entry into this Agreement, the Data Controller accepts that the Data Processor is entitled to change the Subcontracted Data Processors, provided however that a) any new Subcontracted Data Processor complies with the corresponding terms and conditions imposed in this Section 5 on the present Subcontracted Data Processor, and that (b) the Data Controller, at the latest upon commencement of the processing of the personal data that the Data Controller is responsible for, is informed by the Data Processor of the identity of the new Subcontracted Data Processor.

6 Processing and disclosure of personal data to others

6.1 The Data Controller is responsible for ensuring that it has the requisite legal basis for the processing the personal data encompassed within this Agreement.

6.2 The Data Processor may not disclose information to third parties without the written consent of the Data Controller, unless such disclosure is required by law or upon a binding request from a court or data protection authority, or as set out in this Agreement.

7 Security

7.1 The Data Processor is obligated take appropriate technical and organisational security measures to ensure that personal data is not accidentally or unlawfully destroyed, lost or impaired, and precautions to prevent that unauthorised persons gain knowledge of the information, nor that it is misused or otherwise processed in violation of the law, (see Sections 1.2 and 1.3 above).

7.2 The Danish Executive Order on Security (Regulation No. 528 of 15 June 2000 on Security Measures for the Protection of Personal Data that is Processed for the Public Administration, as amended by Regulation No. 201 of 22 March 2001) must also be complied with in situations where the processing of personal data is for public authorities.

7.3 The Data Processor implements and maintains the security measures described in Appendix 1 and in general fulfils the requirements as set forth in the "Terms and Conditions for Hosting." The security requirements as set out in Appendix 1 constitute the Data Controller's security requirements at the Data Processor's premises.

7.4 The Data Processor is entitled at all times to implement alternative security measures, provided that such security measures meet the requirements or provide greater security than those listed in Appendix 1, (see Section 7.3, described security measures) and in general fulfil the requirements in the Hosting Agreement for security. The Data Processor may not, without the Data Controller's prior written consent, impair the security conditions.

7.5 If the Data Processor is established in another EU Member State, the provisions concerning security measures laid down in the legislation of the EU Member State in which the Data Processor is established shall also apply to the Data Processor. If the Data Processor is established in another EU Member State, the Data Processor must comply both with the security requirements encompassed within applicable law in Denmark *and* the security requirements in the Data Processor's home state. The same applies to Subcontracted Data Processors.

7.6 The Data Processor shall, as provided in a more detailed agreement with the Data Controller, assist the Data Controller to the greatest extent feasible in ensuring compliance with the obligations pursuant to Article 32 of the Regulation (Security of processing, implementation of appropriate technical and organisational measures), Article 35 (Data protection impact assessment) and 36 (Prior consultation). In this regard, the Data Processor is entitled to invoice the Data Controller at its customary hourly rate for all the Data Processor's working hours, which such agreement may impose on the Data Processor; the Data Controller is also responsible for any payment to the Subcontracted Data Processors.

7.7 If what is provided in Section 7.6 leads to enhanced security measures in relation to what has already been agreed between the Parties pursuant to this Agreement, the Data Processor shall, as far as possible, implement such measures, provided that the Data Processor receives payment for this (see Section 7.8 below).

7.8 The costs associated with the implementation of such measures (see Section 7.7) are to be borne by the Data Controller, for which the Data Processor has no responsibility. The Data Processor is also entitled to invoice the Data Controller with its customary hourly rate for all the Data Processor's working hours which such implementation may impose on the Data Processor; the Data Controller is also responsible for any payment due to the Subcontracted Data Processor.

8 Right to inspect

8.1 The Data Processor shall provide the Data Controller, upon the request of the Data Controller, with sufficient information so as to ensure that the Data Processor has taken the requisite technical and organisational security measures.

8.2 To the extent that the Data Controller also desires this to include the processing which takes place at the Subcontracted Data Processor(s), the Data Processor will be informed of this. The Data Processor will then obtain sufficient information from the Subcontracted Data Processor(s).

8.3 If the Data Controller desires to carry out an inspection, as stated in this Section 8, the Data Controller shall always provide the Data Processor advance notice of at least 30 days in connection with this.

8.4 If the Data Controller desires to have a security audit report prepared, or in general desires to undertake an inspection of the Data Processor's or Subcontracted Data Processor's processing of personal data, including if the Data Controller desires a security audit report prepared at a specified time, this is to be agreed upon with the Data Processor. The Data Processor, or Subcontracted Data Processor, may insist at any time that such a security audit report be prepared in accordance with a recognised auditing standard (e.g. ISAE 3402 with ISO 27002:2014 or similar as a reference framework) by a generally recognised and independent third party who is customarily engaged with such circumstances.

8.5 The Data Controller is responsible for all costs associated with the security conditions at the Data Processor's premises, as well as in relation to Subcontracted Data Processor(s), including that the Data Processor is entitled to invoice the Data Controller at its customary rate for all the Data Processor's working hours that such inspection may entail the Data Processor to incur; the Data Controller is also responsible for any payments due to the Subcontracted Data Processor(s).

9 Security Breach in the protection of Personal Data

9.1 If the Data Processor becomes aware of a personal data breach, which is understood to mean a breach of security that leads to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to personal data which is transmitted, stored or otherwise processed, the Data Processor is required without undue delay to seek to locate such personal data breaches and to seek to minimise the occurrence of injury to the greatest extent possible, and to the extent it is feasible, to recreate any lost data.

9.2 The Data Processor is also obligated to inform the Data Controller without undue delay after becoming aware that there has been a security breach in the protection of personal data. The Data Processor shall then without undue delay, to the extent this is feasible, notify the Data Controller in writing, including to the extent possible:

9.3 A description of the nature of the personal data breach, including the categories and the approximate number of data subjects affected and personal data registered.

9.4 The name and contact details for the data protection consultant.

9.5 A description of the likely consequences of the data breach.

9.6 A description of the measures the Data Processor, or the Subcontracted Data Processor, has taken (or suggests to be taken) in order to deal with the personal data breach, including measures to limit its possible harmful effects.

9.7 To the extent that it is not possible to provide the information collected as outlined in Section. 9.2, the information may be reported in stages without unnecessary further delay.

9.8 Similarly, Subcontracted Data Processors are required to inform the Data Processor without unnecessary delay in accordance with Sections 9.2 and 9.3.

10 Duty of confidentiality

10.1 The Data Processor must keep the personal data confidential and thus is entitled only to use personal data in the performance of its obligations and rights pursuant to the Agreement.

10.2 The Data Processor must ensure that employees and any others, including Subcontracted Data Processors (subprocessors) authorised to process the Personal Data encompassed within the Agreement, are bound by a duty of confidentiality.

11 Term of the Agreement, and Termination of the Data Processing Agreement

11.1 This Agreement will become effective upon the Parties' signature on the Agreement.

11.2 In the event of the termination of the Hosting Agreement, for whatever reason, the Data Processing Agreement will terminate as well. However, the Data Processor is obligated by this Agreement, as long as the Data Processor processes personal data on behalf of the Data Controller, and the Data Controller shall inform the Data Processor, in writing as soon as possible but no later than 14 days after the termination of the Hosting Agreement, how the Data Processor will manage the processed personal data. 30 days after the termination of the Hosting Agreement, the Data Processor is entitled and obligated to delete all personal data that has been processed under the terminated Hosting Agreement on behalf of the Data Controller.

12 Signature

12.1 The above is accepted, with effect from the date of the signature of the Parties.

12.2 This Agreement has been prepared and signed in two identical copies, with each of the Parties receiving one copy.

For the Customer	For CompuSoft A/S
Date	Date
_____	_____

APPENDIX 1 – DESCRIPTION OF SECURITY MEASURES

1 INTRODUCTION

1.1 This appendix constitutes the appendix referred to in Section. 7.3 in the Data Processing Agreement entered into between Data Processors and Data Controllers for the provision of services.

1.2 The appendix describes the security measures that the Data Controller requires for the physical, technical and organisational security of the Data Processor's delivery of services.

2 PHYSICAL SECURITY

2.1 Fire, power outages, floods, etc. Measures against theft, fire, water, temperature fluctuations and redundancy of electrical power, according to current industry standards.

2.2 Access control Only authorised individuals have access to the premises. External parties, such as suppliers or customers, have access solely in conjunction with authorised individuals.

3 TECHNICAL SECURITY

3.1 Firewalls and anti-virus The systems are protected by firewalls, anti-virus software has been installed on relevant servers and the systems are protected against malicious code execution, in accordance with current industry standards. 15.2 Encryption: All access to the systems, from other locations, is to occur via encrypted connections.

3.2 Backup and Restoration A backup of all servers containing data is to be made daily and the backup is to be replicated to a secondary backup site. Continuous tests are performed on the validity of the backups in the form of restoration checks.

4 ORGANISATIONAL SECURITY

4.1 Access Rights Access accounts are set with differentiated access, so that employees (and customers) only have access to the particular systems and data that is relevant to their work efforts.

4.2 Confidentiality All employees with access to the systems are subject to an obligation of confidentiality via employment contracts or joint collaborative agreements.

5 Logging

5.1 Event logging, personally identifiable logging of the staff operator's access, and proactive logging for monitoring of resource usage, occurs.

6 Deletion and disposal

6.1 All equipment upon which data is saved must be destroyed before disposal.