

## DATA PROCESSING AGREEMENT

BETWEEN DATA DESIGN AS, NORWAY (ORG NO911197146MVA) – *The data "Processor"*  
AND CLIENTS USING THE WEBMERCICS WEBSHOP SOLUTION – *The data "Controller"*

### 1 Introduction, area of application, definitions

- (1) This contract stipulates the rights and obligations of the controller and processor (henceforth referred to as the "Parties") in the context of processing personal data on behalf of the controller.
- (2) This contract applies to all activities for which the processor's employees or any subcontractors that he/she has tasked with processing the controller's personal data.
- (3) The terms used in this contract are to be understood in accordance with their respective definitions in the EU General Data Protection Regulation (GDPR).

### 2 Scope and duration of the data processing

- (1) Scope  
The processor shall carry out the following processes:  
Handling personal data related to e-commerce transactions.  
The processing is based on the pre-existing webshop service contract entered into by the Parties (henceforth referred to as the "Master Contract").
- (2) Duration  
The processing shall begin on the date when the parties sign the Master Contract, or May 25, 2018, whichever is later, and be carried out for an unspecified period until the Master Contract has been terminated by one of the Parties, and the obligations set forth in paragraph 12 are completed.

### 3 Nature and purpose of collecting, processing or using the data

- (1) Nature and purpose of processing the data  
Processing the data consists of the following, but is not limited to: collecting, compiling, organizing, sorting, saving, adapting or changing, separating, recalling, using, publishing or transferring, distributing or any other form of provision, replication or linking, restricting, deleting or destroying data.  
The data is processed for the following purpose: To facilitate receiving and maintaining customer orders in an e-commerce solution.
- (2) Type of data  
The following data is to be processed: customer emails, addresses and other contact information, product selection and preferences, limited payment information.

(3) Categories of persons affected

The following data subjects are affected by the data being processed: Individuals making electronic purchases through the e-commerce solution either for him/herself or for someone they represent (i.e. the company they work for).

#### **4 Obligations of the processor**

- (1) The Processor shall only process personal data as contractually agreed or as instructed by the Controller, unless the Processor is legally obliged to carry out a specific type of data processing. Should the Processor be bound by such obligations, the processor is to inform the Controller thereof prior to processing the data, unless informing him/her is illegal. Furthermore, the Processor shall not use the data provided for processing for any other purposes, specifically his/her own.
- (2) The Processor confirms that he/she is aware of the applicable legal provisions on data protection. He is to observe the principles of correct data processing.
- (3) The processor shall be obliged to maintain strict confidentiality when processing the data.
- (4) Any individuals who could have access to the data processed on behalf of the Controller must be obliged in writing to maintain confidentiality, unless they are already legally required to do so via another written agreement.
- (5) The Processor shall ensure that the individuals he/she employs, who are to process the data, have been made aware of the relevant data protection provisions as well as this contract before starting to process the data. The corresponding training and sensitisation measures are to be appropriately carried out on a regular basis. The Processor shall ensure that the individuals tasked with processing the data are adequately instructed and supervised on an ongoing basis in terms of fulfilling data protection requirements.
- (6) In connection with the commissioned data processing, the Processor must support the Controller when designing and updating the list of processing activities and implementing the data protection assessment. All data and documentation required are to be provided and made available to the Controller upon request.
- (7) Should the Processor be subject to the inspection of supervisory authorities or any other bodies or should affected persons exercise any rights against the Processor, then the Processor shall be obliged to support the Controller to the extent required, if the data being processed on behalf of the Controller is affected.
- (8) Information may be provided to third parties by the Processor solely with the Controller's prior consent, unless the Processor is required by law to supply the data regardless of the Controller's consent. Inquiries sent directly to the Processor will be forwarded to the Controller.
- (9) The Processor shall appoint a professional and reliable individual as the authorised data protection officer.
- (10) Data processing by the Processor is to be carried out in the EU or EEC.

#### **5 Technical and organizational measures**

- (1) The Processor will implement necessary technical and organizational measures for ensuring data protection and data security, including confidentiality, integrity and availability of the

information processed throughout the term of the contract, as well as proper destruction or return of the data to the controller when the contract is terminated.

- (2) The data protection measures may be adjusted according to the continued technical and organizational advancement as long as minimum requirements according to the GDPR have been sufficiently met. The Processor shall immediately implement the changes required for the purposes of maintaining information security. The Controller is to be immediately informed of any changes. Any significant changes are to be agreed upon by the Parties.
- (3) Should the security measures implemented by the Controller not, or no longer, be sufficient, the Processor is to inform the Controller immediately.
- (4) Copies or duplicates are not to be created without the Controller's knowledge. Any technically necessary, temporary duplications are exempt, provided any adverse effects to the agreed upon level of data protection can be ruled out. Examples of such duplications are backups, temporary logs or agreed upon exports to external systems, such as ERP solutions.
- (5) Data processing is only performed at secure data centers
- (6) The Processor shall provide proof of having fulfilled his/her obligations, especially for completely carrying out the necessary technical and organizational measures, upon request.

## **6 Stipulations on correcting, deleting and blocking data**

- (1) In the scope of the data processed on behalf of the Controller, the Processor may only correct, delete or block the data in accordance with the contractual agreement, GDPR requirements, or the Controller's instructions.

## **7 Subcontracting**

- (1) Subcontractors may only be used if they meet the minimum requirements according to the GDPR, and only for supplemental purposes, except with the Controller's written consent.
- (2) Consent is only possible if the subcontractor is subject to a contractual minimum of data protection obligations, which are comparable with those stipulated in this contract. The Controller shall, upon request, inspect the relevant contracts between the Processor and the subcontractor.
- (3) The Processor's and subcontractor's responsibilities must be clearly distinguished.
- (4) The Processor shall choose the subcontractor by specifically considering the suitability of the technical and organizational measures taken by the subcontractor.
- (5) Any transfer of the data processed on behalf of the Controller to the subcontractor shall only be permitted after the Processor has provided convincing documentation that the subcontractor has met his/her obligations in full.
- (6) Appointing any subcontractors, who are to process data on behalf of the Controller, who are not located and do not operate exclusively within the EU or EEC, is only possible if they meet the minimum requirements according to the GDPR.
- (7) The Processor must review the subcontractor's compliance with obligations on a regular basis.
- (8) Subcontracting, in terms of this contract, only refers to those services that are directly associated with rendering the primary service. Additional services, such as transportation, maintenance and cleaning, as well as using telecommunication services or user services, do not apply. The

Processor's obligation to ensure that proper data protection and data security is provided in these cases remains unaffected.

## **8 Rights and obligations of the controller**

- (1) The Controller shall be solely responsible for assessing the admissibility of the processing requested and for the rights of affected parties.
- (2) The Controller shall document all orders, partial orders or instructions. In urgent cases, instructions may be given verbally. These instructions will be immediately confirmed and documented by the Controller.
- (3) The Controller shall immediately notify the Processor if he finds any errors or irregularities when reviewing the results of the processing.
- (4) The Controller shall be entitled to inspect compliance with the data protection provisions and contractual agreements with the Processor to an appropriate extent, either personally or by third-parties, in particular by obtaining information and accessing the stored data and the data processing programs as well as other on-site inspections. The Processor must make it possible for all individuals entrusted with carrying out audits to access and inspect as required. The Processor is required to provide the necessary information, demonstrate the procedures and provide the necessary documentation for carrying out inspections.
- (5) Inspections at the Processor's premises must be carried out without any avoidable disturbances to the operation of his/her business. Unless otherwise indicated for urgent reasons, which must be documented by the Controller, inspections shall be carried out after appropriate advance notice and during the Processor's business hours, and not more frequently than every 12 months. If the Processor provides evidence of the agreed data protection obligations being correctly implemented, as stipulated in chapter 5 (6) of this contract, any inspections shall be limited to samples.

## **9 Notification obligations**

- (1) The Processor shall immediately notify the Controller of any personal data breaches. Any justifiably suspected incidences are also to be reported. Notice must be given to one of the Controller's known addresses within 72 hours from the moment the Processor realizes the respective incident has occurred. This notification must contain at least the following information:
  - a. A description of the type of the personal data protection infringement including, if possible, the categories and approximate number of affected persons as well as the respective categories and approximate number of the personal data sets;
  - b. The name and contact details of the data protection officer or another point of contact for further information;

- c. A description of the probable consequences of the personal data protection infringement;
  - d. A description of the measures taken or proposed by the Processor to rectify the personal data protection infringement and, where applicable, measures to mitigate their possible adverse effects.
- (2) The Controller must also be notified immediately of any significant disruptions when carrying out the task as well as violations against the legal data protection provisions or the stipulations in this contract carried out by the Processor or any individuals he/she employs.
- (3) The Processor shall immediately inform the Controller of any inspections or measures carried out by supervisory authorities or other third parties if they relate to the commissioned data processing.
- (4) The Processor shall ensure that the Controller is supported in these obligations, in accordance with Art. 33 and Art. 34 of the GDPR, to the extent required.

## **10 Instructions**

- (1) The Controller reserves the right of full authority to issue instructions concerning data processing on his/her behalf.
- (2) The Controller may contact the Processor as agreed upon in the Master Contract.
- (3) The Processor shall immediately inform the Controller if an instruction issued by the Controller violates, in his opinion, legal requirements. The Processor shall be entitled to forego carrying out the relevant instructions until they have been confirmed or changed by the party responsible on behalf of the Controller.
- (4) The Processor is to document the instructions issued and their implementation.

## **11 Rights of the Data Subject (henceforth called the "Subject")**

- (1) The Processor is required to be able to fulfill requests from Subjects according to Chapter 3 (Articles 12 to 23) of the GDPR. Such requests include, but are not limited to:
  - a. Right to data portability

The Subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format.
  - b. Right to rectification

The Subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her.
  - c. Right to erasure

The Subject has the right to be forgotten if the personal data are no longer necessary for processing, or other legitimate grounds given in Article 17 of the GDPR applies.

d. **Right to restriction of processing**

The Subject has the right to obtain from the controller restriction of processing based on conditions given in Article 18 of the GDPR.

e. **Right to object**

The Subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her. At the latest at the time of the first communication with the data subject, this right shall be explicitly brought to the attention of the Subject and shall be presented clearly and separately from any other information.

## **12 Ending data processing on behalf of the controller**

- (1) When terminating the contractual relationship or at any time upon the Controller's request, the Processor must either destroy the data processed as part of the commission or submit the data to the Controller at the Controller's discretion. All copies of the data still present must also be destroyed. The data must be destroyed in such a way that restoring or recreating the remaining information will no longer be possible, even with considerable effort.
- (2) The Processor is obligated to ensure the return or deletion of data from subcontractors.
- (3) Any documentation that serves the purpose of providing proof of proper data processing, shall be kept by the Processor according to the respective retention periods, including the statutory period after the contract has expired.

## **13 Liability**

- (1) According to Article 82 of the GDPR, the Controller involved in processing shall be liable for the damage caused by processing which infringes on the GDPR. The Processor shall be liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

## **14 Right to extraordinary termination**

- (1) The Controller may, at any time, terminate the Master Contract and this contract without notice if a serious infringement of data protection regulations or the provisions of this contract exists on part of the Processor, if the Processor cannot or will not execute the client's legal instructions or if the Processor refuses to accept the Controller's supervisory rights, in violation of this contract.

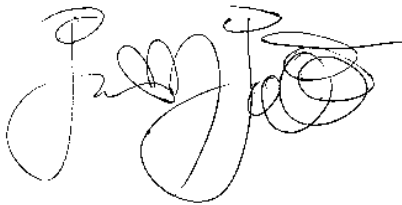
- (2) A serious breach shall, in particular, be deemed to have occurred if the Processor has not substantially fulfilled or failed to fulfill the obligations laid down in this agreement, in particular the technical and organizational measures.
- (3) For insignificant breaches, the Controller shall provide the Processor with a reasonable period of time to remedy the situation. Should the situation not be remedied in good time, the Controller shall be entitled to extraordinary termination as stipulated here.

## 15 Miscellaneous

- (1) Both Parties are obligated to treat all knowledge of trade secrets and data security measures, which have been obtained by the other party within the scope of the contractual relationship, confidentially, even after the contract has expired. If there is any doubt as to whether information is subject to confidentiality, it shall be treated confidentially until written approval from the other party has been received.
- (2) Should the Controller's property be threatened by the Processor by third-party measures (e.g. by seizure or confiscation), by insolvency or settlement proceedings or by other events, the Processor shall immediately notify the Controller.
- (3) Any ancillary agreements must be in writing.
- (4) Should any parts of this agreement be invalid, this will not affect the validity of the remainder of the agreement.

For Data Design AS

Webmercs webshop client

A handwritten signature in black ink, appearing to read 'Joachim Jensrud', with a stylized flourish at the end.

Joachim Jensrud

Authorized representative

Data Protection Officer