Contract on commissioned processing of personal data: controller-processor agreement

Version: 1.0

between

Next Level Escaperoom Eindhoven
Stratumseind 32
De Oude Rechtbank
The Netherlands

Henceforth referred to as **the Controller**

and

SuperSaaS B.V.
Keizersgracht 639
1077 KR Amsterdam
The Netherlands

Henceforth referred to as **the Processor**

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). Furthermore, the declarations may be made in another form under the condition that suitable verification is ensured.

2 Scope and duration of the data processing

2.1 Scope

The Processor shall carry out the following processes:

Provide a web service to allow Controller’s end-users to schedule appointments online. Provide a web service that allows the Controller to manage these appointments and the collected end-user data.

2.2 Duration

Processing shall begin on March 31, 2015 and be carried out for an unspecified period until the SuperSaaS account is deleted by the Controller.

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

3.1 Nature and purpose of processing the data

Processing the data consists of the following: collecting, sorting, saving, transferring, restricting and deleting data

The data is processed for the following purpose: To allow end-users of the Controller to schedule appointments online.

3.2 Type of data

The following data is to be processed:

- Data entered by Controller’s end-users in the process of using the service

3.3 Categories of persons affected

The following data subjects are affected by the data being processed:

- End-users of the online scheduling application of the Controller

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 purpose, 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 immediately available to the Controller upon request.

(7) Should the Controller be subject to the inspection of supervisory authorities or any other bodies or should affected persons exercise any rights against the Controller, 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. Inquiries sent directly to the Processor will be immediately forwarded to the Controller.

(9) If he/she is legally obliged to do so, the Processor shall appoint a professional and reliable individual as the authorised data protection officer. It must be ensured that the officer does not have any conflicts of interest. In the event of any doubts, the Controller can contact the data protection officer directly. The Processor is to then immediately notify the controller of the contact details of the data protection officer or provide a reason as to why a data protection officer has not been appointed. The Processor is to immediately inform the Controller of any changes to the status of the data protection officer or of any changes to his in-house tasks.

(10) Any data processing may only be carried out in the EU or EEC. Any change to a third-party country may take place with the Controller's consent and in accordance with the conditions stipulated in chapter V of the GDPR and this contract.

5 Technical and organisational measures

(1) The data protection measures may be adjusted according to the continued technical and

organisational advancement as long as the agreed upon minimum has 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.

(2) Should the security measures implemented by the Processor not, or no longer, be sufficient, the Processor is to inform the Controller immediately.

(3) 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.

(4) Should the data be processed in a private residence, the Processor is to ensure that a sufficient level of data protection and data security is maintained and that the Controller's supervisory rights as determined in this contract can also be exercised without restriction in the private residence.

(5) Dedicated data media, which originate from the Controller or which are used for the Controller, are to be specifically marked and are subject to ongoing administration. They are to be appropriately stored at all times and must not be accessible to unauthorised persons. Any removals and returns are to be documented.

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 or the Controller's instructions.

(2) The Processor shall comply with the respective instructions provided by the Controller at all times and also after the termination of this contract.

7 Subcontracting

(1) Subcontractors may only be appointed on an individual basis 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 Controller's rights must also be able to be effectively exercised against the subcontractor. In particular, the Controller must have the right to carry out inspections, or have them carried out by third parties to the extent specified here.

(4) The Processor's and subcontractor's responsibilities must be clearly distinguished.

(5) Any additional subcontracting carried out by the subcontractor is not permitted.

(6) The Processor shall choose the subcontractor by specifically considering the suitability of the technical and organisational measures taken by the subcontractor.

(7) 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.

(8) 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 in compliance with the conditions stipulated in chapter 4 (10) of this contract. Specifically, this shall only be permitted if the subcontractor provides appropriate data protection measures. The Processor is to inform the Controller of the specific data protection guarantees provided by the subcontractor and how evidence thereof can be obtained.

(9) The Processor must review the subcontractor's compliance with obligations on a regular basis, every 12 months at the latest. The inspection and its results must be documented such that they are understandable to a qualified third party. The documentation is to be submitted to the Controller without it being requested.

(10) Should the subcontractor fail to fulfil his/her data protection obligations, the Processor will be liable to the Controller for this.

(11) 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 is entitled to appoint a third party independent auditor in the possession of the required professional qualifications and bound by a duty of confidentiality, which auditor must be reasonably acceptable to the Processor, to inspect Processor's compliance with this Data Processing Agreement and the applicable data protection legislation required to determine the truthfulness and completeness of the statements submitted by the Processor under this Data Processing Agreement. Controller's right to audit shall be subject to giving the Processor at least 4 weeks prior written notice of any such audit. The Controller shall bear any and all cost of the audit.

(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, 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 24 hours from the moment the Processor realises 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.

(3) 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.

(4) 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.

(5) 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 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.

(3) The Processor is to document the instructions issued and their implementation.

11 Ending the commissioned processing

(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 immediately 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. The Processor may submit the respective documentation to the Controller once his/her contractual obligations have ended.

12 Remuneration

The Processor's remuneration is conclusively stipulated in the Terms of Use. There is no separate remuneration or reimbursement provided in this contract.

13 Liability

(1) The Controller shall be liable for compensation to anyone for damage caused by any unauthorised party or for incorrect data processing within the scope of the contract.

(2) The Controller shall bear the burden for proving that any damage is the result of circumstances that the Processor is responsible for insofar as the relevant data have been processed under this agreement. If this proof has not been provided, the Controller shall, when initially requested to do so, release the Processor from all claims that are levied against the latter in connection with the data processing.

(3) The Processor shall be liable to the Controller for any damages culpably caused by the Processor, his/her employees or appointed subcontractors or the contract-executing agency in connection with rendering the contractual service requested.

(4) The Processor's liability is limited to the amount paid to the Processor by the Controller in the two years preceding the incident causing the liability

(5) Sections 13 (2) and 13 (3) shall not apply if the damage occurred as a result of correctly implementing the service requested or an instruction provided by the Controller.

14 Right to extraordinary termination

(1) The Controller may, at any time, terminate this contract without notice ("extraordinary termination") 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 fulfil the obligations laid down in this agreement, in particular the technical and organisational 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) Should any parts of this agreement be invalid, this will not affect the validity of the remainder of the agreement.