Definitions

Controller: the natural person or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes of and means for the Processing of Personal Data as referred to in article 4 section 7 GDPR.

Data Subject: the natural person to whom the Personal Data relate, as referred to in article 4 section 1 GDPR.

Data Processing Agreement: this data processing agreement in which the obligations as referred to in article 28 section 3 GDPR are laid down.

Employees: Natural persons working for the Controller or the Processor, whether based on an employment contract or hired on a temporary basis.

GDPR: the General Data Protection Regulation (Regulation (EU) 2016/679), including the implementation Act of this regulation.

Main Agreement: the Main Agreement between the Controller and the Processor, including appendixes, which is governed by this Data Processing Agreement.

Parties: Controller and Processor.

Personal Data: any information relating to an identified or identifiable natural person ('Data Subject') that is processed in the context of the Main Agreement as referred to in article 4 section 1 GDPR; 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: 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 as referred to in article 4 section 12 GDPR.

Processing: any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, 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 as referred to in article 4 section 2 GDPR.

Processor: a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller as referred to in article 4 section 8 GDPR.

Recipient: a natural person or legal person, a public authority, agency or another body, to which the Personal Data are disclosed, whether a third party or not.

Sub-Processor: a different processor who is appointed by the Processor to process Personal Data for the benefit of a Controller.

Data Processing Agreement

Applicability

The controllers and processors listed in **Appendix 4** have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29 (3) and (4) or Regulation (EU) 2018/1725.

This Data Processing Agreement is related to the Processing of Personal Data by the Processor on the instructions of the Controller in the context of the performance of the Main Agreement.

The nature and purpose of the Processing, the type of Personal Data, the categories of Personal Data and Data Subjects and Recipients have been set out in **appendix 1**.

The Processor guarantees that it meets the requirements of applicable rules and regulations on the Processing of Personal Data.

Duration and Termination

This Data Processing Agreement will enter into effect once it is signed by the Parties.

The Data Processing Agreement will end when the Main Agreement ends.

Neither Party has the right to terminate this Data Processing Agreement early without termination of the Main Agreement.

Obligations which by their nature are intended to continue even after termination of this Data Processing Agreement will continue to exist after termination of this Data Processing Agreement. This applies, inter alia, to stipulations arising from provisions on secrecy, liability, dispute resolution and applicable law.

Processing

The Processor will Process the Personal Data exclusively as ordered by and based on written instructions of the Controller, except where otherwise provided by laws that apply to the Processor. The Processor will Process the Personal Data no longer or more extensively than is necessary for the performance of the Main Agreement.

If, in the view of the Processor, an instruction as referred to under the first section of this article is contrary to any statutory regulation on data protection, it will

notify the Controller thereof beforehand, unless a statutory provision prohibits such notification.

If, based on a statutory provision, the Processor is obliged to provide Personal Data, it will notify the Controller thereof immediately, if possible prior to the provision.

The Processor will ensure that only its Employees have access to the Personal Data. The only exception is the appointment of Sub-Processors in conformity with the provisions under article 0 of this Data Processing Agreement. The Processor limits the access of Employees to those for whom access is essential in the performance of their tasks, in which case access is limited to those Personal Data said employees need for the performance of their tasks. The Processor will also ensure that the Employees who have access to the Personal Data have received a correct and full instruction on the handling of Personal Data and that they are aware of the responsibilities and legal requirements.

The Controller is legally obliged to observe prevailing laws and regulations pertaining to privacy. The Controller must in particular verify whether there is question of a legal basis for the Processing of Personal Data. The Processor will ensure that it meets all applicable rules and regulations relating to the Processing of Personal Data, plus the agreements laid down in this Data Processing Agreement.

Processing will take place under the responsibility of the Controller. The Processor does not have any power to decide on the purpose of and means for the Processing and cannot take decisions on matters such as the use of the Personal Data, the retention period of the Personal Data processed for the Controller and the provision of the Personal Data to third parties. The Controller must ensure that the purpose of and means for the Processing of the Personal Data are clearly defined.

Security

The Processor has taken the security measures included in **appendix 2**, which appendix forms part of this Data Processing Agreement. The risks to be mitigated, the state of the art and the costs of security measures have been taken into consideration when defining the security measures. The security measures will in any case include:

- encryption/pseudonymization (encoding) of Personal Data;
- the ability to guarantee permanently the confidentiality, integrity, availability and resilience of processing systems and services;

- the ability to recover quickly the availability of and access to the Personal Data in the event of a physical or technical incident;
- a procedure for the periodical testing, assessment and evaluation of the efficacy of the technical and organisational security measures of Processing.

The Controller is well informed about the security measures taken by the Processor and believes that these measures guarantee an adequate security level in view of the nature of the Personal Data and the size, context, purpose and risks involved in Processing.

The Parties acknowledge that ensuring an adequate security level means that it may continually be necessary to take additional security measures. The Processor will guarantee a security level that matches the actual risks. The Processor will notify the Controller if one of the security measures undergoes a substantial change.

The Processor offers suitable warranties for the implementation of technical and organisational security measures relating to the Processing. If the Controller wishes to inspect or have inspected the compliance by the Processor with the security measures, then the Controller can file a request to that end to the Processor. The Processor and the Controller will make mutual arrangements in this respect. The costs of an inspection must be paid by the Controller. The Controller will make a copy of the inspection report available to the Processor.

Unless with the express written prior permission by the Controller, the Processor will not Process Personal Data or have Personal Data processed by itself or by third parties in countries outside the European Union ("EU").

Confidentiality

All Personal Data received by the Processor from the Controller and/or collected by the Processor itself and/or that the Processor is asked to collect for the purpose of Processing it in conformity with the provisions in the Main Agreement, is subject to a duty of confidentiality vis-à-vis third parties.

The Processor will not use the Personal Data for any other purpose than for which it was received, not even if this data was provided in a form that guarantees that it cannot be traced back to the Controller or any natural person, such as the Data Subject.

The Processor ensures that the individuals who are authorised to Process the Personal Data have undertaken to observe confidentiality or are bound to observe confidentiality pursuant to a relevant statutory obligation.

The obligation to observe confidentiality is not applicable in so far as the Controller or the Data Subject himself/herself has given express permission to transfer the Personal Data to a third party or if and in so far as a legal obligation exists to provide information to a third party.

If the Processor makes use of the services of a Sub-Processor, it will unconditionally ensure that the Sub-Processor accepts in writing the same obligation to observe confidentiality as has been agreed between the Parties and that it will strictly comply with this obligation to observe confidentiality.

Transferability

Unless mutually agreed and laid down in writing, the Parties do not have the right to transfer this Data Processing Agreement and the rights and obligations under this Data Processing Agreement to a third party.

Liability

The Controller ensures that the Processing of Personal Data under this Data Processing Agreement is not unlawful and does not infringe the rights of Data Subjects.

The Processor is liable for the damage or loss of the Controller resulting from the non-performance of this Data Processing Agreement by the Processor or its non-observance of the GDPR or any other relevant rules or regulations.

The limitation of the liability of the Processor as agreed in the Main Agreement with accompanying general terms and conditions applies to all obligations under this Data Processing Agreement.

Obligation to Lend Assistance

The GDPR and other (privacy) laws assign certain rights to Data Subjects. The Processor will lend full and timely assistance to the Controller in the observance of the obligations the Controller has towards Data Subjects.

The Processor will immediately forward to the Controller all complaints received from and all requests made by Data Subjects relating to the Processing of Personal Data.

Upon the Controller's first request, the Processor will provide to the Controller all relevant information on aspects relating to the Processing of Personal Data as performed by it, in such a way that the Controller, partly based on that information, can prove that it meets applicable (privacy) laws.

The Processor will furthermore lend all necessary assistance, upon the Controller's first request, in the observance of legal obligations on the part of the Controller pursuant to applicable privacy laws (including, for example, the performance of a privacy impact assessment). The Processor will have the right to charge the Controller for the assistance provided by it in the context of such requests.

Personal Data Breach

The Processor will notify the Controller without unreasonable delay once it has discovered a Personal Data Breach, in conformity with the agreements as laid down in **appendix 3**. The Processor will make efforts to notify the Controller thereof within 48 hours after having discovered the Personal Data Breach and as soon as possible after the Processor was informed about this by a Sub-Processor.

The Processor will also notify the Controller about any developments relating to the Personal Data Breach as reported by it.

The reporting of a Personal Data Breach to the Data Protection Authority (DPA) and, if relevant, to Data Subjects is at all times the sole responsibility of the Controller.

Keeping a register of Personal Data Breaches is at all times the sole responsibility of the Controller.

Appointment of Sub-Processors

The Processor will not outsource its activities relating to the Processing of Personal Data to a sub-processor without the prior written permission of the Controller.

In so far as the Controller agrees to the appointment of a sub-processor, the Processor will subject this sub-processor to the same or stricter obligations as those that apply to the Processor pursuant to this Data Processing Agreement and the law. The Processor will lay down these obligations in writing and will ensure the compliance thereof by that Sub-Processor. If so requested, the Processor will provide to the Controller a copy of the contract/contracts entered into with the Sub-Processor.

In spite of the permission given by the Controller for contracting a sub-processor that (partly) Processes data on the instructions of the Processor, the Processor will remain fully liable towards the Controller for the consequences of outsourcing work to a sub-processor. The permission of the Controller for the outsourcing of work to a sub-processor does not affect the fact that the appointment of sub-

processors in a country outside the EU requires the permission as referred to under article 0 of this Data Processing Agreement.

Duty of Disclosure and Audits

The Processor will make available all information needed to prove that the obligations under this Data Processing Agreement are and have been met.

The Processor will make available to the Controller all information needed to:

- **prove the observance of the obligations laid down in this Data Processing Agreement, including the obligations as mentioned under articles 0 up to and including 0 of this Data Processing Agreement;**
- **make audits possible, including inspections performed by the Controller or by an inspector authorised by the Controller.**

The Controller will have an audit performed once every year by an Employee of the Controller or by an independent third-party expert.

Return or Deletion

Once this Data Processing Agreement ends, the Processor, at the option of the Controller, will ensure the deletion or the return to the Controller of all Personal Data. The Processor will delete copies, with due observance of applicable legal provisions.

The Processor will delete the Personal Data within 12 weeks after termination of the Data Processing Agreement, failing which the Processor will incur a penalty of € 100 for each day, up to a maximum of € 1.200.

Applicable Law and Competent Court

The Data Processing Agreement is governed by Dutch law.

Disputes on the contents and execution of this Data Processing Agreement will be settled by the Court in the district where the Controller has its registered office.

Appendix 1. Processing of Personal Data

Categories of data subjects whose personal data is processed

- Employees of the controller
- Employees or business partners of the controller
- Users of the products and services that are the subject of the commissioned processing
- Other persons whose data are processed in the course of providing the agreed service

Categories of the personal data processed

- Name
- Contact details
- Contract data
- Invoice data
- Support requests
- Log data
- Personal data contained in financial accounting systems
- Other personal data made available by the controller to the processor in the course of providing the service agreed in the customer agreement

Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

Not applicable

Nature of the processing

- Storage/hosting

Purspose(s) for which the personal data is processed on behalf of the controller

Provision of the service agreed in the customer agreement

- Provision of the software as licensed, configured and used by the controller and its users; troubleshooting (preventing, detection and correction of technical problems); continuous product improvements including provision of updates; ensuring reliability; quality and security of the licensed product

Duration of the processing

The duration of the processing shall be governed by the customer agreement and the instructions of the controller

For processing by (sub-) processors, also specify subject matter, nature and duration of the processing

The controller has authorised the use of the following sub-processors:

- **Name: Amazon Web Services EMEA SARL**

  Address: 38 avenue John F. Kennedy, L-1855, Luxemburg

  Contact person's name, position and contact details: Attn: AWS EMEA Legal

  Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Cloud Services

- **Name: Microsoft Ireland Operations Limited**

  Address: The Atrium Building, Block B, Carmanhall Road, Sandyford Business Estate, Dublin 18, Ireland

  Contact person's name, position and contact details: Attn: Data Privacy, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, D18 P521, Ireland

  Description of the processing (including a clear delimitation of responsibilities in case several sub-processors are authorised): Hosting

Appendix 2: Appropriate Technical and Organisational Measures

Description of the technical and organizational security measures implemented by the processor(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, as well as the risks for the rights and freedoms of natural persons. Examples of possible measures:

Security Guideline Sponsorvista B.V.

Appendix 3: Agreements on Personal Data Breach

If the Processor discovers a breach of the security of Personal Data or a loss of or interference with Personal Data, the Processor will notify the Controller thereof within 24 (twenty-four) hours after the discovery, by means of an e-mail sent to the Controller. In this e-mail, the Processor must in any case indicate that there has been question of a Personal Data Breach, what the (presumed) cause of that Personal Data Breach is, what the (known and/or expected) consequences are, what the (suggested) solution is and which parties have been informed so far.

Appendix 4: List of parties

Controller(s):
Name: Customer (as specified during signup)
Address: as specified during signup
Contact person's name, position and contact details: as specified during signup

Processor(s):
Name: Sponsorvista
Address: Achterhaven 37, 1135XS Edam
Contact: info@sponsorvista.com
Nature of the processing: Provision of the software
Signature and accession date: