Zertic
Terms and Conditions Data processing Agreement

Data processing Agreement

This Data Processing Agreement ("**Agreement**") forms part of the License Contract and Agreement for Zertic Hosted Services ("**Principal Agreement**") between:

4. Client, (**"Data Controller"** or „**Controller**")

AND

Zertic BV., Luchthavenweg 18f, 5657 EB Eindhoven, Netherlands ("**Processor**")

make a Data Processing Agreement in accordance with article 28 of the EC's regulation nr. 2016/679 implemented on April 27th 2016:

WHEREAS

1. The Controller possesses personal data and shares this with the Processor which implies the processing of personal data. The subject of the processing are hosted services as defined in the Principal Agreement.
2. The goal of the processing is to provide hosted services as defined in the Principal Agreement.
3. The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation). The
5. Controller warrants to the Processor that it has the legal right to disclose all Personal Data that it does in fact disclose to the Processor under or in connection with this Agreement, and that the processing of that Personal Data by the Processor for the Permitted Purpose in accordance with this Agreement will not breach any applicable data protection or data privacy laws (including the EU General Data Protection Regulation (GDPR)

The Parties wish to lay down their rights and obligations.

IT IS AGREED AS FOLLOWS:

1. The purpose of the Agreement

1.1 The purpose of the terms of this Agreement is to identify the duties and obligations the Processor has on behalf of the Controller in relations to the Processing that the Principal Agreement specifies.

1.2 The Parties shall be bound by all relevant laws and legislations regarding their Processing of Personal Data, with special emphasis on the EC's regulation nr. 2016/679 of the protection of individuals in relations with the Processing of Personal Data and the free dissemination of that kind of information, and the repeal of directive 95/46/EC (the Data Protection Directive) implemented on May 25th, 2018.

2. Description of the Data Processing the Processor is contracted for.

2.1 The Processor may handle, on behalf of the Controller, the Personal Data needed to provide the services defined in the Principal Agreement.

2.2 The nature of the Processing is storing Personal Data provided by the Controller and implement the Personal Data in queries and other database Processes needed for the services defined in the Principal Agreement.

2.3 The purpose of the Processing is to provide the Controller with an overview of contact information and qualifications of the Controller's staff, committee members and individual contractors and the Controller's clients.

2.4 The Processor is authorized to Process the following types of Personal Data:

(a) Full name

(b) Address and place of residence

(c) Telephone number

(d) Email address

(e) Social Security number (the controller's local SSN equivalent)

(f) Times of user activity

(g) Qualifications / Test results / Certificates

(h) Orders / assignments

(i) Other Personal Data necessary for the services defined in the Principal Agreement.

2.5 The Processor is authorized to Process the Personal Data of the following groups on behalf of the Controller:

(a) Controller 's members of staff

(b) Controller 's individual contractors hired for auditing.

(c) Controller 's committee and working group members.

(d) Controller 's client 's contact persons

2.6 For the Processor to be able to provide the services defined in the Principal Agreement, the Controller shall provide the necessary information to the Processor.

3. Definitions and interpretation

3.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

3.2 "**Agreement**" means this Data Processing Agreement and all Schedules;

3.3 "**Controller Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of Controller pursuant to or in connection with the Principal Agreement;

3.4 "**Contracted Processor**" means both a Processor and Sub-processor;

3.5 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

3.6 "**EEA**" means the European Economic Area;

3.7 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

3.8 "**GDPR**" means EU General Data Protection Regulation 2016/679;

3.9 "Data Transfer" means:

(a) a transfer of Controller Personal Data from the Controller to a Contracted Processor; or

(b) an onward transfer of Controller Personal

Data from a Contracted Processor to a Contracted Processor, or between two establishments of Contracted Processor.

3.10 in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

3.11 "**Services**" means the hosted services the Processor provides as defined by the hosted services specifications in the license contract and agreement.

3.12 "**Sub-processor**" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Controller in connection with the Agreement.

3.13 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor",** and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

4. Duration of the Agreement

4.1 The Agreement is valid for the duration of the Principal Agreement. Written notice shall otherwise be given, honoring the timeframe in clause 12 of this agreement.

5. Obligations of the Processor towards the Controller

5.1 The Processor shall:

(a) Only Process Personal Data in accordance with the purpose of the Processing as defined in this Agreement.

(b) Only Process Personal Data according to written instructions of the Controller, defined in this Agreement. If the Processor believes the instructions of the Controller are not in line with the Personal Data regulation or other appropriate legislation regarding the Processing of Personal Data, the Processor shall report it to the Controller without delay. In addition, the Processor shall report to the Controller if the Processor is by law required to transfer Personal Data to countries outside the EU and/or the European Economic Area (EEA) or international organizations without the

prior written consent of the Controller, unless such reporting is against the law.

(c) Ensure confidentiality regarding the Processing of Personal Data this Agreement covers, and

(d) Ensure that access to the Controller Personal Data is limited to those Processor personnel who have a reasonable need to access the Controller Personal Data to enable the Processor to perform its duties under this Agreement; any access to the Controller Personal Data shall be limited to such part or parts of the Controller Personal Data as are strictly necessary.

(e) Ensure that the employees with access to the Personal Data covered by the Agreement have signed an affidavit of non-disclosure and confidentiality or are bound by professional secrecy by law and will receive adequate training in the protection of Personal Data.

(f) Make sure equipment, products, software, and services are designed with built-in and automatic Personal Data Protection in mind.

6. Use of a Sub-processor

6.1 The processor is authorized to contract a subprocessor for certain parts or elements of the Processing. Before intended changes take place, both when adding a sub-processor and when changing sub-processors already approved, or when the approved Processing done by subprocessors is to be changed, the Processor shall inform the Controller in writing about the change. Specifically, it shall be stated what part of the Processing the sub-processor will handle, the name and contact information of the sub-processor along with the valid dates of the contract. The Controller has 14 days from the day

of receiving the information of the change of subcontracting to protest. The use of the sub-processor is only allowed once the Controller has not protested within the 14-day period.

7. Data Subject Rights.

7.1 Considering the nature of the Processing, the Processor shall assist the Controller by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of the Controller obligations, as reasonably understood by Controller, to respond to requests to exercise Data Subject rights under

the Data Protection Laws.

7.2 The Controller is responsible to inform the individuals about the Processing before or as soon as the Processing starts, in accordance with the Data Protection Law in respect of Controller Personal Data, e.g., article 13 and 14 of the GDPR.

7.3 If the Data Subject requests to exercise their rights with the Processor, the Processor shall forward the request without undue delay to the Controller's Controller Representative as defined in the Principal Agreement. The Processor shall ensure that it does not respond directly to that request except with documented instructions of the Controller or as required by Applicable Laws to which the Processor is subject, in which case Processor shall to the extent permitted by Applicable Laws inform the Controller of that legal requirement before the Processor or SubProcessor responds to the request.

8. Personal Data Breach

8.1 The Processor shall notify the Controller via email without undue delay upon Processor becoming aware of a Personal Data Breach affecting Controller Personal Data, also referring to data loss or destruction, corruption or in any way renders it unusable or the Processor has a reason to suspect that any of the foregoing has occurred The Processor shall provide Controller with sufficient information to allow the Controller to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection and the appropriate authorities.

8.2 The information supplied by the Processor to the Controller shall be simple and concise and describe at a minimum:

8.3 The nature of the breach, including if applicable, groups and a rough estimate of the number of individuals affected by the breach, and the groups and the quantity of Personal Data/records affiliated with the breach.

8.4 The name and contact information of the Personal Data representative or another contact where further information will be available.

8.5 What will be the likely consequences of the breach.

8.6 What counter actions have been implemented or have been planned to implement as a response to the breach, including if applicable, actions intended to minimize the effects on individuals.

8.7 What counter actions individuals can implement to minimize their damage, e.g., change their password.

1.

9. Assistance to the Controller to fulfill the Data Protection Law

9.1 The Processor shall assist the Controller in producing an assessment of the effects of Personal Data Protection.

9.2 The Processor shall provide reasonable assistance to the Controller with any data protection impact assessments, and prior consultations with Supervising Authorities (The controller's Local Data Protection Authority), which the Controller reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Controller Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9.3 In assessing the appropriate level of security, the Processor shall in particular consider the risks that are presented by the Processing, in particular from a Personal Data Breach.

9.4 The Processor shall co-operate with the Controller in relation to:

(a) an investigation into any of the matters in Clause 8(a);

(b) any request from the Controller to amend or delete any of the Controller Personal Data;

(c) any complaint or regulatory notification relating to the processing of any of the Controller Personal Data; and

(d) any request from a data subject for access to any of the Controller Personal Data at the cost and expense of the Controller, except in the case of (a), where the circumstances giving rise to the investigation are the result of the act or omission of the Processor or a security incident affecting the Processor's systems.

10. Security

10.1 The Processor shall create a back-up copy of the Controller Data at least daily, shall ensure that each such copy is sufficient to enable the Processor to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store each such copy for a minimum period of 30 days. The Processor ensures to fulfil these obligations according to the regulations applicable to the country in which the system is hosted.

10.2 Within the period of 1 Business Day following receipt of a written request to the Processor's helpdesk from the Controller, the Processor shall use all reasonable endeavors to restore to the Platform the Controller Data stored in any back-up copy created and stored by the Processor in accordance with Clause 11.3.

10.3 The Controller acknowledges that this process will overwrite the Controller Data stored on the Platform prior to the restoration. Except where the need to restore the Controller Data arises out of an act or omission of the Processor this service will be invoiced by the Processor to the Controller. If the service can't be fulfilled in time, the service is free as is the license fee for the downtime period

11. Data Transfer

11.1 The Processor may not transfer or authorize the transfer of Data to countries outside the EU and/or the European Economic Area (EEA) without the prior written consent of the Controller.

11.2 If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected.

11.3 To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. Deletion or return of Controller Personal Data

12.1 Following the termination of the Principal Agreement, and within 5 Business Days following the date of receipt of a written request from the other party ("Cessation date"), the relevant party shall destroy or return to the other party (at the other party's option) all media containing the other party's Confidential Information and shall irrevocably delete the other party's Confidential Information from its computer systems.

12.2 Processor shall provide written certification to Controller that it has fully complied with this section within 5 business days of the Cessation Date.

13. Representatives for Personal Data Protection

13.1 Representatives for Personal Data Protection shall be the same at the respective representatives defined in the Principal Agreement.

14. Records of processing activities

14.1 The Processor shall keep a record of the Processing it handles for the Controller. The following shall be included at a minimum:

14.2 the names and contact information of the Processor and relevant sub-processors, Controller, and its representative.

14.3 The categories of Processing it handles for the Controller.

14.4 If applicable, the dissemination of Personal Information to countries outside of the EU or EEA, international organizations, or if the dissemination falls under the GDPR's article 49, paragraph 1, subparagraph 2 regarding suitable protective arrangements.

14.5 If possible, a general description of the technical and organizational safety precautions mentioned in article 32(1) of the GDPR.

15. Audit rights

15.1 Subject to this section, the Processor shall make available to the Controller on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Controller or an auditor mandated by the Controller in relation to the Processing of the Controller Personal Data by the Contracted Processors.

15.2 Information and audit rights of the Controller only arise under section 15.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

16. Obligations of the Controller to the Processor

16.1 The Controller shall:

(a) hand over to the Processor the Data

referred to in chapters 2.4 and 2.5 of this document.

(b) document in writing all requests regarding the Processing meant for the Processor.

(c) ensure, before and after the Processing, the Controller works in accordance with the obligations and requirements bestowed upon them by the GDPR, and

(d) oversee the Processing, including auditing the Processor.

17. General Terms

17.1 **Confidentiality:** Each Party shall keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and shall not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

(a) disclosure is required by law;

(b) the relevant information is already in the public domain.

17.2 **Notices:** All notices and communications given under this Agreement shall be in writing and will be delivered personally, sent by post, or sent by email to the address or email address set out in the heading of this Agreement at such other address as notified from time to time by the Parties changing address.

18. Governing Law and Jurisdiction

18.1 This Agreement is governed by Dutch laws.

18.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the controller's national court.