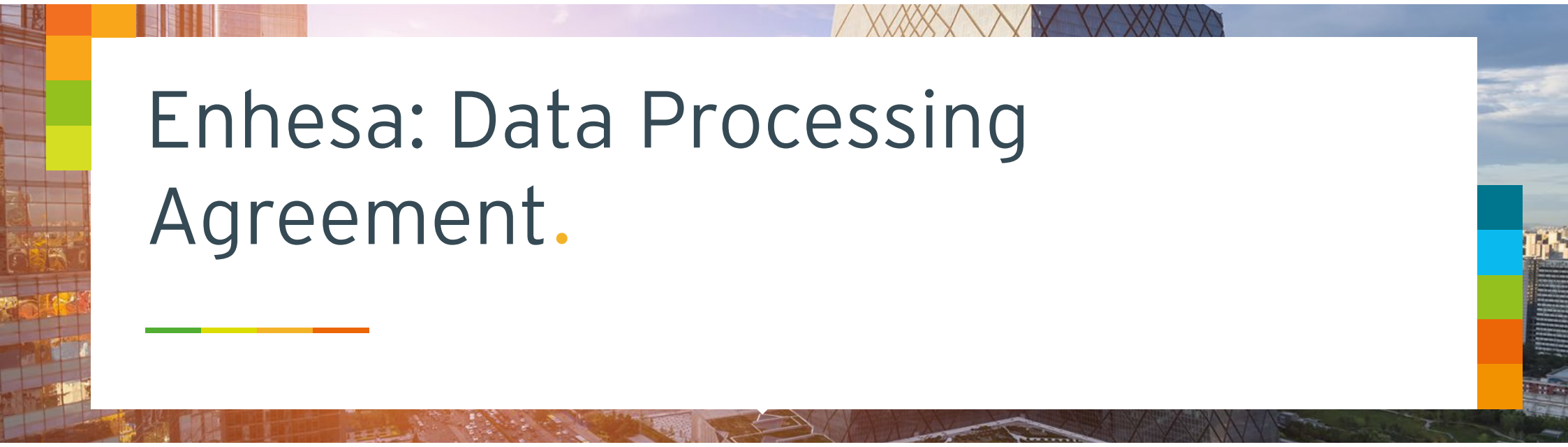

Enhesa: Data Processing Agreement.

ENHESA DATA PROCESSING ADDENDUM

To the extent that Enhesa Processes Personal Data, on behalf of the Customer through providing the Services, and the Data Protection Legislation applies to such Processing, this Data Processing Addendum hereinafter set forth, as amended from time to time, shall form a part of the Enhesa Master Services Agreement (MSA) between Customer and Enhesa and is hereby incorporated by reference into the Agreement, without the need for further action. In case of conflict between the Provisions of the Agreement and this DPA, the provisions of the DPA shall prevail.

1 Definitions and Interpretation

1.1 Capitalized terms used, but not defined, in this Data Processing Addendum are defined in the Agreement, the other capitalized terms used in this Data Processing Addendum shall have the following meaning:

1.1.1 "**DPA**" means this Enhesa Data Processing Addendum together with its annexes, which shall be an integral part of the Agreement between the Parties.

1.1.2 "**Services**" means the services provided by Enhesa including the Services (as defined in the Agreement) and Consulting Services.

1.1.3 "**Sub-processor**" means any Processor (including any third party excluding a person working under the authority of Enhesa) appointed by or on behalf of Enhesa, or its Sub-processor, to Process Personal Data on behalf of Enhesa in connection with the Agreement.

2 Object of this DPA

2.1 This DPA is added to the Agreement in order to comply with applicable Data Protection Legislation, and the provisions of the Agreement shall apply to this DPA.

2.2 For the purposes of this DPA End-Users, as detailed in the Agreement shall be considered to form an integral part of the Customer and Customer shall be responsible for their compliance with this DPA.

2.3 This DPA sets out the subject-matter and duration of the Processing, the nature and purpose(s) of the Processing, the types of Personal Data and categories of Data Subjects and the obligations and rights of the Customer and Enhesa in relation to the Services as further detailed in **Annex I** (Details of Processing).

3 Duration and Termination

3.1 The duration of the Processing is set out in the Agreement.

3.1 The duration of the Processing is set out in the Agreement.

3.2 Upon termination or expiry of this DPA, or at any earlier moment if the Processing of Personal Data is no longer relevant for the delivery of the Services, Enhesa shall delete the Personal Data unless a law or regulation requires storage of the Personal Data.

3.3 Notwithstanding the foregoing, articles 3, 4 and 5 of this DPA shall survive the termination of this DPA.

4 Data Protection

4.1 Parties shall comply with the applicable Data Protection Legislation, for their own account and sole responsibility, unless otherwise set out herein.
account and sole responsibility, unless otherwise set out herein.

4.2 Where Personal Data is Processed by Enhesa in relation to the performance of this DPA, the Agreement and the Services, Enhesa shall:

4.2.1 **Instructions –** process the Personal Data only on documented instructions from Customer as solely provided herein, unless required to do so by applicable laws and regulations to which Enhesa is subject. In such a case, Enhesa shall inform Customer of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. Parties agree that this DPA makes up the entire instruction of Customer to Enhesa, any other instructions have to be agreed to in writing by Enhesa, reserving its rights to charge additional costs for compliance with such instructions;

4.2.2 **Need-to-know –** provide Personal Data only to authorised persons (which shall include employees, agents, resellers, distributors, partners, Sub-processors and subcontractors) on a need-to-know basis and ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

4.2.3 **Measures –** taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account in particular the risk of accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to the Personal Data. A description of the Enhesa requirements as further detailed in Annex II (Security Requirements). Such requirements and measures may be updated by Enhesa, from time to time. Customer shall be solely responsible for its own means of accessing the Services (e.g. through proxies) and providing adequate measures to ensure an appropriate level of security;

4.2.4 **Sub-processors –** based on the general authorisation to use Sub-processors hereby provided by Customer, inform Customer of any addition or replacement of Sub-processors, thereby giving Customer the opportunity to object to such changes on reasonable grounds during a period of ten (10) days, after which such Sub-processors shall be deemed to have been accepted. A description of the Enhesa Sub-Processors is further detailed in Annex III (Sub-processors). Sub-processors engaged by Enhesa prior to entering into this DPA are accepted by Customer. In case Customer objects to a new Sub-processor and such objection is based on reasonable grounds, Enhesa shall employ reasonable efforts to resolve the issue.

Where Enhesa engages a Sub-processor for carrying out specific Processing activities on its behalf, reasonably equivalent data protection obligations as set out in this DPA shall be imposed on that Sub-processor. Where that Sub-processor fails to fulfil its obligations under the Data Protection Legislation, Enhesa shall remain fully liable to Customer in accordance with the terms set out in this DPA;

4.2.5 **Assistance –** taking into account the nature of the processing, reasonably assist Customer by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of Customer's obligation to respond to requests for exercising Data Subject's rights, without prejudice to Enhesa' right to charge Customer any reasonable costs for such assistance. Enhesa shall promptly notify Customer about any legally binding request by a Data Subject;

4.2.6 **Cooperation –** reasonably assist Customer in ensuring compliance with its obligations relating to the: security of the Processing, notification of Personal Data Breaches and data protection impact assessments and prior consultations taking

into account the nature of Processing and the information available to Enhesa and without prejudice to Enhesa' right to charge Customer any reasonable costs for such assistance;

4.2.7 **Personal Data Breach –** Enhesa shall notify the Customer without undue delay after becoming aware of a Personal Data Breach. Such notification shall contain following information: (i) the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (ii) the name and contact details of the data protection officer or other contact point where more information can be obtained; (iii) the likely consequences of the Personal Data Breach; (iv) the measures taken or proposed to be taken by Enhesa to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

The obligation to report or respond to a Personal Data Breach is not and will not be construed as an acknowledgement by Enhesa of any fault or liability with respect to the Personal Data Breach;

4.2.8 **Information & Audit –** make available to Customer all information reasonably necessary to demonstrate compliance with the obligations laid down in this DPA and allow for and contribute to audits, including inspections subject to following conditions. Customer must request an audit in writing and with prior notice of thirty (30) calendar days and may instruct acknowledged audit professionals at its own expense to execute such audit in following cases:

- once every twelve (12) months provided that such additional audit inquiries shall not unreasonably impact in an adverse manner Enhesa' regular operations and do not prove to be incompatible with applicable legislation or with the instructions of a competent authority;
- Where an audit is reasonably considered necessary because of genuine concerns as to Enhesa' compliance with this DPA;
- Where a competent data protection authority requires this under applicable Data Protection Legislation;
- Following a Personal Data Breach.

  The Customer shall promptly notify Enhesa with information regarding any non-compliance discovered during the course of an audit or review of provided information. The Customer agrees to provide Enhesa with a draft of the audit report for review. Enhesa is entitled to propose any amendments and add management comments to this draft before Customer establishes the final version.

4.2.9 reasonably inform Customer if, in its opinion, an instruction infringes applicable Data Protection Legislation.

4.3 **Transfer –** Personal Data Processed in the context of this DPA may be transferred to a country outside the European Economic Area without the prior written consent of Customer, where Enhesa ensures that appropriate safeguards are in place for such transfer or an adequate level of protection is guaranteed. Customer hereby authorises Enhesa to enter into Standard Contractual Clauses (SCC's) within the meaning of article 46(2) (c) & (d) GDPR, on behalf of Customer. For the sake of clarity in such case, Customer shall be the data exporter (as defined in the SCC's) and Enhesa or its Sub-processor shall be the data importer (as defined in the SCC's).

5 Privacy Statement

5.1 Without prejudice to Section 2.1, Enhesa may Process certain Personal Data for its own purposes (e.g. execution of the Agreement), such Processing shall not be subject to this DPA. In such cases Enhesa shall be considered a controller, for more information please refer to our privacy policy: https://www.enhesa.com/privacy-policy.

List of Annexes

- Annex I: Details of Processing
- Annex II: Security Requirements
- Annex III: Sub-processors

Annex I: Details of Processing

1. **The duration of the Processing**

   The duration of the Processing is set out in this DPA.
2. **The subject-matter of the Processing**

   The subject-matter of the Processing is set out in this DPA and relates to the Services.
3. **The types of Personal Data to be Processed**

   All data collected through or by the Services, which includes: user's first and last name, user's email address and company name
4. **The categories of Data Subjects to whom the Personal Data relates**

   The Personal Data may relate to Customer, End-Users and/or any other Data Subject to whom the data may relate as provided by Customer.
5. **The nature and purpose of the Processing**

   Enhesa may Process Personal Data on behalf of Customer through i.a. recording, storage, adaption, transmission & dissemination, in provision of the Services.

Annex II: Security Requirements

Enhesa has implemented appropriate technical and organizational measures to ensure a level of security appropriate to the risk, taking into account in particular the risk of accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to data, which meet following requirements:

<u>Organizational requirements:</u>

- Security policy
- Appointment internal responsible for information security / data protection
- Asset Management
- Staff Training
- Classification of information
- Periodic verification of the adequacy of the processing systems and services
- Processing register
- Infringement log

<u>Technical requirements:</u>

- Backup system
- Access control (physical and logical)
- Authenticate & Authorization
- Password policy
- Logging system, detection and analysis of access
- Anti-virus
- Fire wall
- Network security
- Supervision, review and maintenance of the systems
- Encryption of company data and user's password
- ISO 27001 Certification

Annex III: Sub-processors

Sub-processor	**Service Description**	**Incorporation Location**	**Storage / Transfer Location**	**Transfer Justification**

Microsoft, Inc. (Azure)	Cloud storage	United States	United States	SSC's & EU-US Privacy shield
Microsoft, Inc. (Azure)	Enhesa platform hosting	United States	West Europe	SSC's & EU-US Privacy shield
Sentia Belgium NV	Enhesa platform hosting	Belgium	Storage: Belgium	ISO 27001 certified