Data Processing Agreement

This Data Processing Agreement (including its appendices and annexes, the "**DPA**"), as may be updated from time to time to fully comply with changing regulations, are incorporated by default and form part of the entire Agreement(s) between Parties as defined below, unless specifically stated otherwise.

1. Purpose and Scope

This DPA describes the Parties' obligations, including under applicable privacy, data security, and data protection laws, with respect to the processing and security of Customer Data (as defined below). This Addendum will be effective on the Effective Date of the Agreement between Parties, for the duration of the Agreement.

2. Definitions

"**Agreement**" means the contract under which Enhesa has agreed to provide the applicable Services to Customer.
"**Applicable Privacy Law**" means, as applicable to the processing of Customer Personal Data, any national, federal, European Union, state, provincial or other privacy, data security, or data protection law or regulation.
"**Customer Data**", has the meaning defined in the Agreement.
"**Customer Personal Data**" means the personal data contained within the Customer Data, including any special categories of personal data or sensitive data defined under Applicable Privacy Law.
"**Data Incident**" means a breach of Enhesa's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Enhesa.
"**GDPR**" means, as applicable: (i) the EU GDPR; i.e. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, or (ii) the UK GDPR.
"**European Data Protection Law**" means, as applicable: (a) the GDPR; or (b) the Swiss FADP.
"**Services**" means the services as described in the Agreement.
"**Subprocessor**" means a third party authorized as another processor under this Addendum to process Customer Data in order to provide parts of the Services or to host Enhesa's software solutions.
"**Supervisory Authority**" means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; or (b) the "Commissioner" as defined in the UK GDPR or the Swiss FADP.
"**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

3. Duration

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Enhesa deletes all Customer Data as described in this Addendum.

4. Roles of Parties – Processing details

4.1 Enhesa NV is a processor, and Customer is a controller or processor, as applicable, of Customer Personal Data.

4.2 The subject matter and details of the processing of Customer Personal Data are as follows:

a. The data collected through or by the Services only includes business personal information, i.e. user's first and last name, user's email address and company name.

b. 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.

d. The nature and purpose of the Processing includes Enhesa processing Personal Data on behalf of Customer through i.a. recording, storage, adaption, transmission & dissemination, in provision of the Services.

4.3 Each party will comply with its obligations related to the processing of Customer Personal Data under Applicable Privacy Law.

5. Data Processing

5.1 Customer instructs Enhesa to process Customer Data in accordance with the applicable Agreement (including this Addendum) and applicable law only as follows: (i) to provide, secure, and monitor the Services; and (ii) as further specified via Customer's use of the Services, any other instructions given by Customer and acknowledged by Enhesa as constituting instructions under this Addendum. Customer shall give instructions in writing or in a machine-readable format (in text form*). Customer shall, without undue delay, confirm in writing or in text form any instruction issued orally.

5.2 Enhesa will comply with the Instructions unless prohibited by European Law, where European Data Protection Law applies, or prohibited by applicable law, where any other Applicable Privacy Law applies.

5.3 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. The processing generally takes place within the EU and within the European Economic Area (EEA). Any transfer to a third country may take place only with the express consent of the Company and is subject to the conditions in Chapter V of the GDPR and must be in compliance with the provisions of this Agreement.

6. Data Deletion

Upon request by Customer made within one-hundred eighty (180) days after any expiration or termination of the Agreement, Enhesa shall provide Customer a file of all Customer Data in a standard machine-readable format. After such one-hundred eighty (180) day period, Enhesa will have no obligation to maintain or provide any Customer Data and may thereafter, unless legally prohibited, delete, wipe or otherwise purge all Customer Data.

7. Data Security

7.1 Enhesa's Security Measures, Controls and Assistance.

7.1.1 Enhesa will implement and maintain technical, organizational, and physical measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. The Security Measures include measures to encrypt Customer Data at rest and in transit; to help ensure ongoing confidentiality, integrity, availability and **resilience** of Enhesa's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Enhesa may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

Security measures take into account the state of the art, the costs of implementation, 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. Customer shall be solely responsible for its means of accessing the Services (e.g. through proxies) and providing adequate measures to ensure an appropriate level of security;

The data security measures referred to in Annex 2 of Appendix 2 – Standard Contractual Clauses are mandatory. They define the minimum owed by the Processor. The description of the measures must be sufficiently detailed as to enable a knowledgeable third party to recognize beyond a doubt at any time, on the basis of the description alone, what the required minimum should be.

7.1.2 Organizational requirements are as follows:

a. security policy

b. appointment internal responsible for information security / data protection

c. asset management staff training

d. classification of information

e. periodic verification of the adequacy of the processing systems and services

f. processing register

g. infringement log

7.1.3 Technical requirements are as follows:

a. backup system

b. access control (physical and logical)

c. authenticate & authorization

d. password policy logging system

e. detection and analysis of access

f. anti-virus firewall network security

g. supervision, review and maintenance of the systems

h. encryption of company data and user’s password

i. sub-processing and data hosting exclusively by ISO 27001 certified providers”

7.1.4 Access and Compliance.

Enhesa will (a) authorize its employees, contractors and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions, (b) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance; and (c) ensure that all persons authorized to process Customer Data are under an obligation of confidentiality.

7.1.5 The processing of data in private homes is forbidden.

7.2 Data Incidents.

7.2.1 Enhesa will notify Customer without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize harm and secure Customer Data.

7.2.2 Enhesa’s notification of a Data Incident will describe: the nature of the Data Incident, the measures Enhesa has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Enhesa recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Enhesa's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3 Enhesa's notification of or response to a Data Incident under this Section will not be construed as an acknowledgement by Enhesa of any fault or liability with respect to the Data Incident.

7.3 Customer's Security Responsibilities and Assessment.

7.3.1 Without prejudice to Enhesa's obligations under Sections 7.1 and 7.2, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Enhesa's or Enhesa's Subprocessors' systems, including:

a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. backing up or retaining copies of its Customer Data as appropriate.

7.3.2 Customer agrees that the Services and Security Measures provide a level of security appropriate to the risk to Customer Data

7.4 Compliance Certifications.

Enhesa will supply, on simple written demand, all relevant ISO- and any additional certifications as well as penetration testing ("Pentest") reports produced by Enhesa's accredited Third-Party Auditor and updated annually (the "Pentest Reports").

Enhesa may replace a Compliance Certification with an equivalent or enhanced alternative.

7.5 Reviews and Audits of Compliance.

To demonstrate compliance by Enhesa with its obligations under this Addendum, Enhesa will make the Security Documentation and Pentest Reports available for review by Customer, on Customer demand.

8. Assistance to Customer

Enhesa will assist Customer in ensuring compliance with its obligations relating to data protection assessments, risk assessments, prior regulatory consultations or equivalent procedures under Applicable Privacy Law, by:

a. making the Security Documentation available;

b. providing the information contained in the applicable Agreement (including this Addendum); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9. Access – Data Subject Rights – Data Export

9.1 Access; Rectification; Restricted Processing; Portability.

During the Term, Enhesa will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, and to export Customer Data. If

Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be able to rectify that data.

9.2 Data Subject Requests.

9.2.1 During the Term, if Enhesa receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Enhesa will (i) advise the data subject to submit their request to Customer, (ii) promptly notify Customer; and (iii) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request.

9.2.2 Enhesa will, upon Customer's request, provide Customer with additional reasonable cooperation and assistance.

10. Data Processing Locations

Customer Data may be processed in any country where Enhesa or its Subprocessors maintain facilities. The locations of Enhesa and sub-processors' data centers is described in Section 11.

11. Subprocessors

Customer specifically authorizes Enhesa's engagement as Subprocessors of these entities:

Sub-Processor	Service Description	Incorporation	Server Location	Transfer Justification
Microsoft, Inc. (Azure)	Cloud storage	United States	European Union	SCCs & EU-US Data Privacy Framework
Microsoft, Inc. (Azure)	Enhesa platform hosting	United States	European Union	SCCs & EU-US Data Privacy Framework
Amazon Web Services, Inc.	Cloud storage & platform hosting	United States	United States	SCCs & EU-US Data Privacy Framework
CW Research Ltd. *(wholly owned subsidiary)*	Regulatory content analysis & support services	United Kingdom	European Union	UK Data Protection Act
Enhesa, Inc. *(wholly owned subsidiary)*	Regulatory content services & client support	United States	European Union	SCCs & EU-US Data Privacy Framework
Scivera LLC *(wholly owned subsidiary)*	Regulatory content development	United States	European Union	SCCs & EU-US Data Privacy Framework
RegScan LLC *(wholly owned subsidiary)*	Regulatory content development	United States	European Union	SCCs & EU-US Data Privacy Framework
Nihon Enhesa KK *(wholly owned subsidiary)*	Localized content support	Japan	European Union	European Commission adequacy decision (23/01/2019)
Enhesa (Shanghai) Co. Ltd. * *(wholly owned subsidiary)*	*Limited support services only. No storage or independent access to production personal data.*	PRC	European Union	SCCs & PRC PIPL Security Assessment
Enhesa NV – Sucursal em Portugal	Branch of Enhesa NV	Portugal	European Union	Not applicable

* *Note regarding PRC-based sub-processor:*
Enhesa (Shanghai) Co. Ltd. provides limited support functions under strict internal controls. It does not independently store or access production environments containing personal data. Data transfers are subject to EU Standard Contractual Clauses (SCCs) and security assessments in compliance with the PRC Personal Information Protection Law (PIPL). Technical and organizational safeguards are in place to ensure data protection equivalence.

In addition, Customer generally authorizes Enhesa's engagement of other third Parties as Subprocessors under the condition that when engaging any Subprocessor, Enhesa will

(a) ensure via a written contract that

(i) the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so per the applicable Agreement (including this Addendum); and

(ii) if required under Applicable Privacy Laws, the data protection obligations described in this Addendum are imposed on the Subprocessor and

(b) remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

(c) The engagement of Subprocessors who carry out commissioned processing in territories other than the territory of the EU or the EEA shall be possible only if the conditions set out Clause 5.3 of this DPA are observed. In particular, it is only permissible as far and as long as the Subprocessor offers appropriate data protection safeguards. The Processor shall inform the Customer of the specific data protection safeguards offered by the Subprocessor and how a confirmation of such safeguards may be obtained. Insofar as currently valid standard contractual clauses based on a decision of the EU Commission (e.g. under Commission Decision 2010/87/EU) or standard data protection clauses in terms of Art. 46 of the GDPR are used as appropriate safeguards, the Customer will grant the Processor, with exemption from the prohibition of double representation pursuant to § 181 of the German Civil Code (BGB), the authority to perform all actions necessary for this and to grant and receive declarations of intent for and from the Subprocessor. Furthermore, the Processor is empowered to exercise the rights and authority granted to the Customer by this Agreement against the Subprocessor.

Enhesa shall specifically inform the Customer in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the Customer sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). Enhesa shall provide the Customer with the information necessary to enable the Customer to exercise its right to object. If no objection is made within the aforementioned period, this shall be deemed to constitute the Customer`s consent to the use of this sub-processor.

12. Records Retention

Enhesa will keep appropriate documentation of its processing activities as required by Applicable Privacy Law. Enhesa may make any such information available to competent regulators, including a Supervisory Authority, if required by Applicable Privacy Law.

13. Notices

Notices under this Addendum (including notifications of any Data Incidents) will be delivered to the contact details in the Agreement.

14. Privacy Statement

Enhesa may Process certain Personal Data for its own purposes (e.g. execution of the Agreement) and 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 located at https://www.enhesa.com/privacy-policy

Appendix 1 – Specific Privacy Laws

The terms in each subsection of this Appendix apply only where the corresponding law applies to the processing of Customer Personal Data.

1. European Data Protection Law

1.1 Additional Definitions.
"**Adequate Country**" means:

(a) for data processed subject to the EU GDPR: the European Economic Area, or a country or territory recognized as ensuring adequate protection under the EU GDPR;

(b) for data processed subject to the UK GDPR: the UK, or a country or territory recognized as ensuring adequate protection under the UK GDPR and the Data Protection Act 2018; or

(c) for data processed subject to the Swiss FADP: Switzerland, or a country or territory that is: (i) included in the list of the states whose legislation ensures adequate protection as published by the Swiss Federal Data Protection and Information Commissioner, if applicable; or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FADP;

in each case, other than on the basis of an optional data protection framework.

"**Alternative Transfer Solution**" means a solution, other than SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.

"**Customer SCCs**" means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor), or the SCCs (Processor-to-Controller), as applicable.

1.2 Customer's Audit Rights.
Enhesa will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections). During such an audit, Enhesa will make available all information necessary to demonstrate compliance with its obligations under this Addendum.

1.3. Data Transfers.
The Parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection Law applies to the transfers of these European ("**Restricted Transfers**"), then:

a. if Enhesa has adopted an Alternative Transfer Solution for any Restricted Transfers, Enhesa will inform Customer of the relevant solution and ensure that such Restricted Transfers are made in accordance with it; or

b. if Enhesa has not adopted an Alternative Transfer Solution for any Restricted Transfers, or informs Customer that Enhesa is no longer adopting, an Alternative Transfer Solution for any Restricted Transfers (without adopting a replacement Alternative Transfer Solution):

i. if Enhesa's address is in an Adequate Country:

A. the SCCs (Processor-to-Processor, Enhesa Exporter) will apply with respect to such Restricted Transfers from Enhesa to Subprocessors; and

B. in addition, if Customer's billing address is not in an Adequate Country, the SCCs (Processor-to Controller) will apply (regardless of whether Customer is a controller or processor) with respect to such Restricted Transfers between Enhesa and Customer; or

ii. if Enhesa's address is not in an Adequate Country, the SCCs (Controller-to-Processor) or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller or processor) with respect to such Restricted Transfers between Enhesa and Customer.

1.4 Certification by Non-EMEA Customers.

If Customer's billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, Customer will certify as such and identify its competent Supervisory Authority.

1.5 Information about Restricted Transfers.

Enhesa will provide Customer with information relevant to Restricted Transfers, Additional Security Controls and other supplementary protective measures.

1.6 SCC Audits.

If Customer SCCs apply, Enhesa will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs.

1.7 SCC Notices.

Customer will forward to the relevant controller promptly and without undue delay any notice that refers to any SCCs.

1.8 Termination Due to Data Transfer Risk.

If Customer concludes, based on its current or intended use of the Services, that appropriate safeguards are not provided for transferred Customer Personal Data, then Customer may immediately terminate the applicable Agreement in accordance with that Agreement's termination for convenience provision or, if there is no such provision, by notifying Enhesa.

1.9. No Modification of SCCs.

Nothing in the Agreement (including this Appendix) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

1.10 Precedence of SCCs.

To the extent of any conflict or inconsistency between any Customer SCCs (which are incorporated by reference into this Appendix) and the remainder of the Agreement (including this Appendix), the Customer SCCs will prevail.

1.11 Requirements for Subprocessor Engagement.

European Data Protection Law requires Enhesa to ensure via a written contract that the data protection obligations described in this Addendum, as referred to in Article 28(3) of the GDPR, if applicable, are imposed on any Subprocessor engaged by Enhesa.

2. CCPA

2.1 Additional Definitions.

"**CCPA**" means the California Consumer Privacy Act of 2018, as amended, including as amended by the California Privacy Rights Act of 2020, together with all implementing regulations.

"**Customer Personal Data**" includes "personal information".

The terms "**business**", "**business purpose**", "**consumer**", "**personal information**", "**processing**", "**sale**", "**sell**", "**service provider**", and "**share**" have the meanings given in the CCPA.

2.2 Prohibitions.

Without prejudice to Enhesa's obligations under Section 5 of this DPA, with respect to the processing of Customer Personal Data in accordance with the CCPA, Enhesa will not, unless otherwise permitted under the CCPA:

a. sell or share Customer Personal Data;

b. retain, use or disclose Customer Personal Data:

i. other than for a business purpose under the CCPA on behalf of Customer and for the specific purpose of performing the Services and TSS; or

ii. outside of the direct business relationship between Enhesa and Customer; or

c. combine or update Customer Personal Data with personal information that Enhesa receives from or on behalf of a third party or collects from its own interactions with the consumer.

2.3. Compliance.

Without prejudice to Enhesa's obligations under Section 5 or any other rights or obligations of either party under the applicable Agreement, Enhesa will notify Customer if, in Enhesa's opinion, Enhesa is unable to meet its obligations under the CCPA, unless such notice is prohibited by applicable law.

2.4 Customer Intervention.

If Enhesa notifies Customer of any unauthorized use of Customer Personal Data, Customer may take reasonable and appropriate steps to stop or remediate such unauthorized use by:

a. taking any measures recommended by Enhesa, if applicable; or

b. exercising its rights pertaining to Customer Audit or the Access; Rectification; Restricted Processing; Portability section.

Appendix 2 – Standard Contractual Clauses
(Module 2 – Controller to Processor)

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council Of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) ([1]) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I. A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation(EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Clause 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9 – Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Clause 18(a) and (b).

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([4]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefiting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defense of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorization for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and tIextent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorizing access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved, and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorizing access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([12]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary, with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Belgium.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Belgium.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[2] Not applicable

[3] Not applicable

[4] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[5] Not applicable

[6] Not applicable

[7] Not applicable

[8] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[9] Not applicable

[10] Not applicable

[11] Not applicable

[12] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: **Customer**, as specified in the Agreement

Address: As specified in the Agreement.

Contact person's name, position and contact details: Contact details for the data exporter are specified in the Agreement, where such details have been provided by the data exporter.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services to the data exporter in accordance with the Agreement. Those Services may include advisory, consulting or implementation services if ordered by the data exporter from the data importer in relation to Enhesa's Services.

Signature and date: The parties agree that execution of the Agreement and certification by the data exporter in relation to Enhesa's Services under Section 4.2 of the European Data Protection Law, as applicable, shall constitute execution of these Clauses by both parties.

Role (controller/processor): controller

Data importer(s):

Name: **Enhesa**

Address: As specified in the Agreement.

Contact person's name, position, and contact details: dpo@enhesa.com.

Activities relevant to the data transferred under these Clauses: The data importer provides the Services, including any applicable Implementation Services, to the data exporter in accordance with the Agreement.

Signature and date: The parties agree that execution of the Agreement and certification by the data exporter in relation to Enhesa's Services under Section 4.2 of the European Data Protection Law terms of the CDPA (Customers) or CDPA (Partners), as applicable, shall constitute execution of these Clauses by both parties.

Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects are the individuals whose personal data is processed by the data importer under the data exporter's instructions as specified in the Agreement ("Transferred Personal Data"). These individuals may include, for example: employees, other staff such as contractors and temporary workers, customers and clients (including their staff), other end users, suppliers (including their staff), relatives and associates of the above, advisers, consultants and other professional experts, shareholders, members or supporters, and students and pupils.

Categories of personal data transferred

Transferred Personal Data may include, for example:

- Personal details, including any information that identifies the data subject and their personal characteristics, including: name, address, contact details.

Nature of the processing

The data importer will process Transferred Personal Data to provide, secure and monitor the Services in accordance with the Agreement.

Purpose(s) of the data transfer and further processing

The data importer will process Transferred Personal Data to provide, secure and monitor the Services in accordance with the Agreement.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

The data importer will retain Transferred Personal Data until its deletion in accordance with the provisions of the Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
As above.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

Belgian Data Protection Authority (GBA), an independent body of the federal Parliament which ensures compliance with the fundamental principles of the protection of personal data.
Address: Rue de la Presse 35, 1000 Brussels
Telephone number: +32 (0)2 274 48 00
Company number: 0694.679.950.

ANNEX II
TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA
The data importer will implement and maintain security standards at least as protective as those set out in the Data Processing Addendum and in **Provider Compliance Contract - Appendix 1 of the Master Service Agreement** for any Services, as applicable.

Further measures:

<u>Procedures for regular testing, assessment and evaluation (Art. 32 (1) (d) GDPR, Art. 25 (1) GDPR)</u>

- Data Protection Management
- Incident Response Management
- Data Protection by Design and Default (Art. 25 (2) GDPR)
- Order or Contract control

ANNEX III – LIST OF SUB-PROCESSORS

Sub-Processor	Service Description	Incorporation	Server Location	Transfer Justification
Microsoft, Inc. (Azure)	Cloud storage	United States	European Union	SCCs & EU-US Data Privacy Framework
Microsoft, Inc. (Azure)	Enhesa platform hosting	United States	European Union	SCCs & EU-US Data Privacy Framework
Amazon Web Services, Inc.	Cloud storage & platform hosting	United States	United States	SCCs & EU-US Data Privacy Framework
CW Research Ltd. *(wholly owned subsidiary)*	Regulatory content analysis & support services	United Kingdom	European Union	UK Data Protection Act
Enhesa, Inc. *(wholly owned subsidiary)*	Regulatory content services & client support	United States	European Union	SCCs & EU-US Data Privacy Framework
Scivera LLC *(wholly owned subsidiary)*	Regulatory content development	United States	European Union	SCCs & EU-US Data Privacy Framework
RegScan LLC *(wholly owned subsidiary)*	Regulatory content development	United States	European Union	SCCs & EU-US Data Privacy Framework
Nihon Enhesa KK *(wholly owned subsidiary)*	Localized content support	Japan	European Union	European Commission adequacy decision (23/01/2019)
Enhesa (Shanghai) Co. Ltd. * *(wholly owned subsidiary)*	*Limited support services only. No storage or independent access to production personal data.*	PRC	European Union	SCCs & PRC PIPL Security Assessment
Enhesa NV – Sucursal em Portugal	Branch of Enhesa NV	Portugal	European Union	Not applicable

* *Note regarding PRC-based sub-processor:*
Enhesa (Shanghai) Co. Ltd. provides limited support functions under strict internal controls. It does not independently store or access production environments containing personal data. Data transfers are subject to EU Standard Contractual Clauses (SCCs) and security assessments in compliance with the PRC Personal Information Protection Law (PIPL). Technical and organizational safeguards are in place to ensure data protection equivalence.

ANNEX IV

SUPPLEMENTARY TERMS FOR SWISS FADP TRANSFERS ONLY

The following terms supplement the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to the Swiss FADP:

1. References to the GDPR will be interpreted as references to the Swiss FADP, to the extent applicable.
2. References to the EU and EU Member States will be interpreted to mean Switzerland, to the extent applicable.
3. The term ’Member State’ will be interpreted in such a way as to allow data subjects in Switzerland to exercise their rights under the Clauses in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the Clauses.
4. The competent supervisory authority/ies for purposes of Annex I.C (Competent Supervisory Authority) of the Clauses will be the Federal Data Protection and Information Commissioner in Switzerland (or its replacement or successor).

ANNEX V

SUPPLEMENTARY TERMS FOR UK GDPR TRANSFERS ONLY

The following United Kingdom International Data Transfer Addendum to the European Commission Standard Contractual Clauses supplements the Clauses only if and to the extent the Clauses apply with respect to data transfers subject to the UK GDPR.

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part I - Tables

Table 1: Parties

Start date	(a) 21 September 2022, where the effective date of the Agreement is before 21 September 2022; or (b) otherwise, on the effective date of the Agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: Customer Trading name (if different): As specified in the Agreement. Main address (if a company registered address): As specified in the Agreement. Official registration number (if any) (company number or similar identifier): As specified in the Agreement.	Full legal name: Enhesa Trading name (if different): As specified in the Agreement. Main address (if a company registered address): As specified in the Agreement. Official registration number (if any) (company number or similar identifier): As specified in the Agreement.
Key Contact	Contact details for the data exporter are specified in the Agreement. Details about the data exporter's data protection officer are available to the data importer in the Admin Console for Enhesa Cloud Platform, Enhesa Workspace or Cloud Identity (where such details have been provided by the data exporter).	Contact details for the data importer are specified in the Agreement. The data importer's data protection team can be contacted At dpo@enhesa.com
Signature (if required for the purposes of Section 2)	The Parties agree that execution of the Agreement and certification by the data exporter in relation to Enhesa's Services under Section 4.2 of the European Data Protection Law terms of the Cloud Data Processing Addendum (Customers) or the Cloud Data Processing Addendum (Partners), as applicable, shall constitute execution of this Addendum by both Parties.	The Parties agree that execution of the Agreement and certification by the data exporter in relation to Enhesa's Services, shall constitute execution of this Addendum by both parties.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: 4 June 2021 Reference (if any): Module 2: Controller-to-Processor Other identifier (if any): N/A

Table 3: Appendix Information

"*Appendix Information*" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Annex I(A)

Annex 1B: Description of Transfer: Annex I(B)

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Annex II

Annex III: List of Subprocessors (Modules 2 and 3 only): Annex III

Part 2: Mandatory Clauses

Mandatory Clauses	Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

Part 3: Supplementary Clauses

Supplementary Clauses	Supplementary Clauses of the Approved Addendum, being the following: The data importer may not end this Addendum as set out in Section 19 of the Mandatory Clauses unless the data importer has adopted an Alternative Transfer Solution for the Restricted Transfers by the end date. An "Alternative Transfer Solution" for this purpose means a solution, other than Standard Contractual Clauses, that enables the lawful transfer of personal data to a third country in accordance with Chapter V of the UK GDPR. Any written notice provided by the data exporter pursuant to Section 19 of the Mandatory Clauses in order to end this Addendum will be deemed to terminate the Agreement for convenience.