Addendum: Data Processing Agreement

This Addendum is a part of the Terms and Conditions, Collaboration Agreement and any other written or electronic agreement between NUCLEUS NV (Hereafter: "**Data Processor**") and its customers with regards to the processing of personal data. By agreeing with this Addendum, the customer (Hereafter: "**Data Controller**") enters into a DPA on behalf of itself and, to the extent required under the Applicable Law, on behalf of its Authorized Affiliates.

In this Addendum Data Controller and the Data Processor may be referred to individually as a "**Party**" and collectively as the "**Parties**".

Whereas:

- Data Controller wishes to subcontract certain services, which imply the Processing of Personal Data, to the Data Processor.
- Parties seeks 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 natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), which will serve as an Addendum to the Terms and Conditions, Collaboration Agreement and any other written or electronic agreement with the Data Processor to the extent that it is related to the processing of Personal Data.
- Parties consider proper Processing of Personal Data to be highly important and hereto have agreed to enter into this Data Processing Agreement, which governs the Parties' rights and obligations with regard to the Processing of Personal Data.

It is agreed as follows:

1. Definitions

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

Personal Data, Special Categories of Data, Processing/Process, Data Processor, Data Controller and Data Subject shall have the same meaning as stated in the General Data Protection Regulation.

Applicable Law: European Union or Member State law applicable to the Processing of Personal Data, including, to the extent applicable, any other relevant regulations, guidelines, policies, instructions or recommendations of any governmental authority and any amendments, replacements updates, or later versions thereof;

Data Breach: a breach of security that poses a risk to the rights and freedoms of Data Subjects with regard to their Personal Data or leads to serious, negative consequences for the protection of Personal Data;

Data Processing Agreement ("DPA"): this Addendum including its recitals and any accompanying appendices;

Data Protection Authority: the relevant statutory authority in each jurisdiction where NUCLEUS processes Personal Data or where the Data Controller is established;

Employees: the persons engaged by a Party for the implementation of this Data Processing Agreement, who will operate under the responsibility of the Party;

Sub-processor: any legal person appointed by a Party or a Party's affiliate which processes Personal Data on behalf of one or both Parties in connection with the Collaboration Agreement and this Data Processing Agreement.

Online Data Register: the data register that needs to be maintained by the Data Controller through the control panel login given to the Data Controller by the Data Processor.

2. Object of this Data Processing Agreement

2.1. The Data Controller is any natural person or company, organization or any legal entity that wishes to use the services of the Data Processor. Data Controller determines the purposes and means for the Processing of Personal Data.

2.2. The Data Processor is NUCLEUS NV. Data Processor offers Hosting Services which will be defined as set forth in the Terms and Conditions to which the Data Controllers must agree in order to use the services of the Data Processor. Data Processor will process the Personal Data on behalf of and for the benefit of Data Controller. Data Processor will process the Personal Data to offer its Services to Data Controller.

2.3. For the full duration of the Collaboration Agreement between Parties and this DPA the processing of the transferred Personal Data will be limited to the services offered by the Data Processor as set forth in the Terms and Conditions, under section 3 'Hosting Services'.

2.4. Data Controller and Data Processor shall perform the services in accordance with the provisions of the DPA and the Applicable Law.

2.5. Data Processor undertakes to exclusively process the personal data of

Data Subjects gathered by the Data Controller according to its purpose as set forth by the Data Controller. The rightful acquisition of personal data from data subjects is the exclusive responsibility of the Data Controller. The data processed by the Data Processor commissioned by the Data Controller is set forth in the Online Data Register.

2.6. The transferred Personal Data concern, but are not limited to the categories of Data Subjects, the categories of Data and the special categories of Data as described in the Online Data Register, which Data Controller must keep up to date. An update of the transferred data must occur at least six (6) months after the last update. It is the sole responsibility of the Data Controller to keep the Online Data Register up to date. If the Data Controller fails to provide the Data Processor with the accurate information through the Online Data Register, he will bear all responsibility for the consequences.

2.7. This DPA shall enter into force between Parties at the moment of acceptation of the Terms and Conditions, or any other agreement concerning the processing of Personal Data and shall remain active until the main agreement between Parties is terminated. This agreement cannot be terminated separately. After termination of this agreement, the Data Processor shall still adhere to some provisions such as data breach notification and confidentiality.

3. Rights and obligations of Parties

3.1. Parties explicitly agree to protect the privacy of the Data Subjects and to comply with the relevant provisions of the Applicable Law and the obligations as laid down in this DPA.

3.2. Each Party shall promptly notify the other Party in the event that it is unable to comply with any of its obligations under this DPA.

3.3. Parties guarantee that the Personal Data shall only be provided to those Employees who need access to the data for the performance of their duties and only on a need to know basis, to the extent necessary to fulfil their job requirements. If the Employees are involved in any Processing of the Personal Data, Parties will correctly inform their Employees. Parties will be responsible for the compliance of their Employees with the Applicable Law and this DPA, specifically regarding the security and confidentiality obligations.

<u>Rights and obligations of the Data Controller</u>

3.4. Data Controller determines the purposes and means for the Processing of the Personal Data and has instructed and, throughout the duration of the Collaboration Agreement, will instruct the Data Processor to Process the transferred Personal Data only on the Data Controller's behalf and in accordance with the Applicable Law.

3.5. Data Controller warrants that the Processing of Personal Data is not illegal, will not be used for any illegal activities and does not violate the rights of Data Subjects. The Data Controller is responsible for the collected data, even if the Data Processor helped with the processing of Personal Data.

3.6. Data Controller warrants that it has implemented technical and organizational security measures before Processing the transferred Personal Data.

3.7. Data Controller shall inform, if the transfer involves special categories of Personal Data, the Data Subjects about the Processing of their Personal Data to the extent that sufficient transparency is offered. Data Controller also ensures that parental notice and consent will be obtained before Processing of the Personal Data.

3.8. Data Controller warrants that if the Data Subject invokes any rights according to the Applicable Law and/or claims compensation for damages under this DPA, the Data Processor cannot be held responsible, except for breaches solely caused by Data Controller in which case penalties are limited to the amount set forth in the main services contract.

<u>Rights and obligations of the Data Processor</u>

3.9. Data Processor shall process the Personal Data on behalf of the Data Controller only to provide its services as specified in the Collaboration Agreement and this DPA.

3.10. Data Processor will not rent, sell, or share received Personal Data with third parties, unless it is required for sub-processing. Data Processor may make anonymous data available to third parties. This will always take place in accordance with the Applicable Law.

3.11. Data Processor warrants that it has implemented technical and organizational security measures before Processing the transferred Personal Data. The Data Processor ensures that there are adequate guarantees through ISO 27001 certification. The Data Processor undertakes to adhere to every security measure within the ISO 27001 and undertakes to implement all those security measures to guarantee the safe processing of personal data.

3.12. Data Processor warrants to deal promptly with all inquiries from the Data Controller relating to its Processing of the Personal Data and to abide by the advice of the supervisory authorities with regard to the Processing of the Personal Data.

3.13. Data Processor will promptly notify the Data Controller about any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, any accidental or unauthorized access, and any request received directly from the Data Subjects.

3.14. Data Processor will process the Personal Data on behalf of Data Controller as long as necessary for the execution of the Collaboration Agreement and subsequently this DPA. After this period, the Personal Data will be destroyed or made anonymous.

3.15 Data Processor will assist the Data Controller in complying with requests and demands of Data Subject in the execution of their rights under the General Data Protection Regulation.

4. Sub-processing

4.1. The Data Processor shall not subcontract any of its Processing operations performed on behalf of the Data Controller without the prior written consent of the Data Controller. Where the Data Processor subcontracts its obligations under the Collaboration Agreement, with the consent of the Data Controller, it shall do so only by way of a written agreement with the Sub-processor which imposes the same obligations on the Sub-processor as are imposed on the Data Processor under this DPA.

4.2. When Processing operations are subcontracted to a Sub-processor, the Data Processor shall remain the contact point at all times.

Transfer of Personal Data outside the European Economic Area

4.3 Parties have the right to use Subcontractors of their choice and can choose to subcontract its Processing activities outside the European Economic Area (EEA) to the extent permitted by the Applicable Law. Parties shall only choose a Subcontractor of a country outside the EEA that offers an adequate protection level for Personal Data. Where the transfer is to a Subcontractor in the United States of America, such safeguards shall in particular result from the EU-US Privacy Shield self-certification scheme.

4.4 Nucleus, in its role of Data Processor, undertakes to never share any personal data outside of the European Economic Area (EEA). In addition, Nucleus undertakes to keep all the processed personal data in Belgium to enforce its obligation so have adequate organisational and technical measures to safely process personal data.

5. Cooperation with supervisory authorities

5.1. The Data Controller agrees to deposit a copy of this DPA with the supervisory authority if it so requests or if such deposit is required under the Applicable Law.

5.2. Parties agree that the supervisory authority has the right to conduct an audit of the Data Controller Data Processor and of any Sub-processor.

6. Security measures

6.1. Parties shall take the appropriate and necessary technical and organizational security measures compliant with the Applicable Law to safeguard Personal Data against destruction, either by accident or unlawful, loss, forgery, disclosure, unauthorized distribution, transfer or access, especially when Processing data includes transmission through a network or against any other improper use. Parties will implement and will continue to implement those measures to prevent unauthorised or unlawful Processing or accidental loss or destruction of the Personal Data that is Processed.

6.2. Data Controller will take all necessary protection measures conform the required standards as laid down in the Applicable Law and where deemed necessary will do this by a variety of security technologies and procedures, such as making the Personal Data anonymous or encrypted if needed. The determination of the relevant measures takes into account the state of the art, the cost of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects. Parties agree that this is an obligation of means.

6.3. Parties will continuously ensure that the Processing systems used meet the requirements of confidentiality, integrity and availability. Parties will also check whether their systems are sufficiently resilient, which means that recovery is quick after temporary unavailability.

Reporting of Data Breaches

6.4. Parties shall maintain adequate procedures designed to detect and respond to a Data Breach, including procedures for preventive and corrective actions.

6.5. If the Data Processor determines a Data Breach, it will report this to the Data Controller without undue delay. The notification shall include all necessary information as follows from the Applicable Law, such as the nature and the scope of the Data Breach, its consequences and the proposed and/or taken measures to remedy and/or limit the consequences.

6.6. When a Data Breach occurred the Data Controller is responsible to take action. This includes taking all adequate measures to remedy and limit the consequences without any delay as well as the necessary measures to avoid reoccurrence, all at its own costs. Data Controller is responsible to notify the personal Data Breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it.

7. Confidentiality

7.1. Parties acknowledge that they may become privy to confidential information which is disclosed by the other Party.

7.2. Parties shall not disclose confidential information to any third party and shall not use confidential information for any purposes other than for the purposes of this DPA. Parties shall safeguard the confidential information to the same extent that they safeguard their own confidential information and in any event with no less than a reasonable degree of protection.

7.3. This confidentiality obligation also explicitly applies to the Parties' employees and Sub-processors.

7.4. This obligation does not apply when a Party is permitted or required to disclose this information by law, a supervisory authority, law enforcement agencies, public authority, arbitrator or court order, when the information is publicly known or when the data is provided on behalf of a Party. Parties will inform each other in such event.

7.5. This obligation of confidentiality will continue to apply after termination of this DPA.

8. Liability

8.1. Parties agree that if one Party is held liable for a violation of the clauses of this DPA committed by the other Party, the latter will, to the extent to which it is liable, indemnify the first Party for any cost, charge, damages, expenses or loss it has incurred.

8.2. Indemnification is contingent upon the Data Controller promptly notifying the Data Processor of a claim; and the Data Processor being given the possibility to cooperate with the Data Controller in the defence and settlement of the claim.

9. Terms and termination

9.1. This DPA enters into force on the date that the Data Processor first provides its Services to Data Controller in the performance of the Collaboration Agreement. In order to fully implement and/or develop the necessary security measurements, standards and requirements, a two month implementation period shall be taken into account upon signing this DPA.

9.2. This DPA shall remain in force and effect until the Collaboration Agreement is terminated or expired, unless Parties agree that earlier termination is required to comply with the requirements of the Applicable Law or a decision of a supervisory authority or court order.

9.3. After termination of the Collaboration Agreement and this DPA, the Data Processor will immediately cease and desist all Processing of Personal Data with regard to its Services. In addition, on request Data Processor provides all the information and documents needed for the subsequent Processing of the data. This disclosure of information is done in good faith.

9.4. Any obligation arising from this DPA that by nature has post-contractual effect, shall continue to be in effect after the termination of this DPA.

10. Miscellaneous

10.1. This DPA together with the Collaboration Agreement constitutes the entire agreement and understanding between the Parties with respect to its subject matter and replaces all previous agreements between, or understandings by, the Parties with respect to such subject matter. In the event of any conflict or inconsistency between the terms of this DPA and those of the Collaboration Agreement or the Terms and Conditions specifically regarding the Processing of Personal Data of Data Subjects, the terms of this DPA shall be decisive to the extent necessary to resolve the conflict.

10.2. Deviations from and additions to this DPA shall only be valid by written instrument signed on behalf of both Parties.

10.3. In the event that one or more provisions of this DPA turn out not to be legally valid or not enforceable, the specific provision(s) will be modified to the minimum extent necessary to make the provision(s) valid, legal and enforceable. Parties will negotiate in good faith to amend the provision so that it, to the greatest extent possible, achieves the intended commercial result of the original provision. If such modification is not possible, the relevant (part of the) provision shall be deemed deleted. Any modification or (partly) deleting of a provision shall not affect the validity and enforceability of this DPA.

11. Applicable Law and Jurisdiction

11.1. Data Controller agrees that if the Data Subject invokes any rights and/or claims compensation for damages under this DPA, the Data Controller will accept the decision of the Data Subject to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority or to refer the dispute to the Belgian courts.

11.2. Parties acknowledge that this DPA is governed by Belgian law. Any disputes arising within the scope of this DPA may only be brought before the competent courts of the judicial district of Antwerp.