ADDENDUM GENERAL DATA PROTECTION REGULATION

BETWEEN:

WOLTERS KLUWER BELGIUM NV, with registered offices at 2800 Mechelen, Motstraat 30,
RPR Antwerpen, division Mechelen, VAT BE 0405.772.873,

Hereinafter referred to as "**the Controller**"

AND:

Name + legal entity form, with registered offices at address,
VAT BE number,

Duly represented by **name,** function

Hereinafter referred to as "**the Processor**"

Hereinafter jointly also to be referred to as the "**Parties**" and each separately as a "**Party"**

On date Parties have concluded an agreement regarding subject/title (hereinafter referred to as "**the Agreement**") and have agreed to comply with their obligations under the General Data Protection Regulation 2016/679 of April 27th, 2016 by signing present addendum (hereinafter referred to as **"the Addendum"**).

PARTIES HAVE AGREED AS FOLLOWS:

Articlel 1 Definitions

Terms such as "processing", "personal data", "data subject", "controller" and "processor" shall have the meaning ascribed to them in i) up to 25 May 2018, the Data Protection Directive 95/46/EC; and (ii) from 25 May 2018 onwards, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation: "**GDPR**").

Article 2 Subject of this Addendum

2.1 This Addendum applies exclusively to the processing of personal data within the framework of the Agreement.

2.2 During the performance of the Agreement, the Processor may process personal data ("**Personal Data**") on behalf of and on instructions from the Controller in the course of the performance of the Agreement with the Controller. An overview of the categories of Personal Data, the purposes for which they are being processed and a description of the processing operation(s) are included in Annex 1 to this Addendum. The Controller shall be solely responsible for determining the purposes for which and the manner in which Personal Data are, or are to be, processed.

2.3 The ownership of the Personal Data that are being processed by the Processor shall remain with the Controller, unless the processing pertains to Personal Data of the Processor or its personnel.

Article 3 Execution of Processing

3.1 The Processor will act as the processor and the Controller will act as the controller.

3.2 The Processor warrants that it will only process the Personal Data on behalf of the Controller in a manner that is necessary for the performance of the Agreement. Other processing operations will only be executed on written instructions of the Controller or if there is a statutory requirement to do so. The Processor shall never process the Personal Data for any purposes of its own or that of others.

3.3 The Processor shall follow all reasonable instructions of the Controller in connection with the processing of the Personal Data in accordance with this Addendum and the Agreement. If the Processor is required to process the Personal Data as a result of EU or member state law to which the Processor is subject, the Processor shall inform the Controller of that legal requirement before processing. The Processor shall immediately inform the Controller if in its opinion instructions are in conflict with the applicable laws with regard to the processing of personal data or with the Agreement between the Parties.

The Processor shall notify the Controller immediately and in writing when the Controller or a third party on behalf of the Controller provides, transfers or makes visible Personal Data which the Processor reasonably is not allowed to receive within the framework of the Agreement or any binding legal provision, with particular attention to sensitive data (Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation or criminal convictions and offences or related security measures)

3.4 The Processor shall process the Personal Data demonstrably, in a proper and careful manner and in accordance with its obligations as a processor pursuant to the GDPR. The Processor shall also adhere to the stipulations that apply to the Controller pursuant to the appropriate national or local data protection laws.

3.5 The Parties conclude the Agreement and this Addendum in order to profit from the expertise of the Processor concerning the securing and processing of the Personal Data for the purposes set out in Annex 1 of this Addendum. The Processor will, at his own expense, implement and maintain appropriate technical and organisational measures to protect the Personal Data at all times against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure, access, or processing. The Processor shall be allowed to use such tools as it considers necessary to pursue those purposes.

3.6 The Processor shall, at his own expernse, fully cooperate with the Controller to:

(i) allow the data subjects access to their Personal Data after approval and by order of the Controller,

(ii) delete or correct Personal Data or to provide Personal Data tot he data subjects in a transmittable format,

(iii) to process any data subject requests regarding, amongst others, objection against direct marketing, profiling for direct marketing or individual automised decision making,

(iv) prove that Personal Data have been deleted or corrected if they are incorrect (or, in the event that the Controller does not agree to the Personal Data being incorrect, to establish the fact that the data subject considers its Personal Data to be incorrect),

(v) assist the Controller with any Data Protection Impact Assessment as required by Art. 35 of the GDPR that relates to the services provided by the Processor to the Controller and the Personal Data Processed by the Processor on behalf of Controller, and

(vi) otherwise give the Controller the opportunity to meet its obligations under the GDPR or other applicable laws in the field of personal data processing.

3.7 The Processor shall store and process the Personal Data concerning the Controller strictly separately from the Personal Data it processes for itself or on behalf of third parties.

Article 4 Data transfers

4.1 The Processor shall immediately notify the contact person of the Controller as mentioned in Annex 2 of any (planned) permanent or temporary transfers of Personal Data to a country outside the European Economic Area without an adequate level of protection and shall only perform such (planned) transfers after obtaining written consent and instruction of the Controller and if all legal requirements are met.

4.2 Annex 1 provides a list of transfers for which the Controller grants its consent upon the conclusion of this Addendum.

The Controller shall at all times have the right to attach additional conditions to its consent to such processing. Where that consent is given it may be conditional on any export being done on the terms of a binding agreement incorporating the EU standard clauses entered into between the Controller and the Processor. The Processor agrees to accept any modifications to such standard clauses which are necessary to comply with laws applicable to such data transfer. Such binding agreement shall be without prejudice to the rights of the Controller under this Addendum.

Article 5 Confidentiality

5.1 Without prejudice to any other contractual confidentiality obligations of the Processor, the Processor warrants that it shall treat all Personal Data as strictly confidential and that it shall inform all its employees, agents and/or approved sub-processors engaged in the processing of the Personal Data of the confidential nature of such information and of the Personal Data. The Processor shall ensure that all persons and parties have signed appropriate contractual confidentiality, data protection and data security obligations, which are at least as restrictive as this Addendum and that they will comply with the provisions of this Addendum. The Processor shall provide the Controller with copies of these agreements upon request. The Processor shall not be permitted to show, provide or otherwise make available the Personal Data to any third party, unless this is necessary or permitted pursuant to the Agreement as mentioned in Article 2 and included under Annex 1, or in the event that explicit prior written consent has been obtained from the Controller to do so.

5.2 The Parties shall treat all information the Processor has to provide to the Controller by virtue of Article 6 and Article 7 of this Addendum as strictly confidential.

Article 6 Security & Verification of Personal Data

6.1 Without prejudice to any other security standards agreed upon elsewhere by the Parties, the Processor shall demonstrably, in accordance with the current ISO/IEC 27001 standard (i.e. the standard for information security), take appropriate technical and organisational security measures, which considering the current state of the art and the accompanying costs are in accordance with the nature of the Personal Data to be processed, in order to protect the Personal Data at all times against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, access or unlawful processing. These measures shall include in any case:

a) measures to ensure that the Personal Data can be accessed only by authorized personnel who need to access the Personal Data for the purposes set forth in Annex 1 of this Addendum;

b) measures to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;

c) measures to identify vulnerabilities with regard to the processing of the Personal Data in the systems used to provide services to the Controller;

d) the measures agreed upon by the Parties in Annex 4.

6.2 The Processor shall at all times have in place an appropriate, written security policy with respect to the processing of Personal Data, outlining in any case the measures as set forth in Article 4.1. At the request of the Controller, the Processor shall provide a copy of such security policy, shall demonstrate the measures it has taken pursuant to this Article 6 and shall amend its security policy in accordance with the Controller's further written instructions.

6.3 The Controller has the right to audit and test compliance with the measures mentioned above under the Articles 6.1 and 6.2. Such audit will be performed by an independent third party. At the request of the Controller, the Processor shall in any case give the Controller the opportunity to do this once a year at a time to be decided by the Parties in mutual consultation or, if the Controller deems this necessary as a result of (suspected) data or privacy incidents. The Processor shall duly comply with any instructions given by the Controller as a result of such monitoring to amend the security policy.

6.4 The Processor shall cooperate and make available to the Controller at its own costs all information requested by the Controller to demonstrate the Processor's compliance with the obligations set out in this Data Processor Agreement, in particular in respect of the inspection mentioned under Article 6.3.

6.5 The Controller will bear the costs for the audit, unless the audit shows that the Processor does not comply with the Addendum. In such case, the Processor bears the costs of the audit.

6.6 The Parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Processor will therefore constantly evaluate the measures as implemented on the basis of this Article 4 and will tighten, supplement or improve these measures in order to keep meeting its obligations under this Article 6.

6.7 The Controller has the right to instruct the Processor to take additional security measures. Where an amendment to the Agreement is necessary in order to execute such an instruction, the Parties shall negotiate an amendment to the Agreement in good faith.

Article 7 Monitoring, Information Obligations and Incident Management

7.1 The Processor shall actively monitor for any breaches of the security measures and shall report the results of the monitoring to the Controller in accordance with this Article 7 within the terms set by law.

7.2 As soon as any incident with regard to the processing of the Personal Data occurs, has occurred or could occur relating to security measures, the Processor is obliged to at all times notify the Controller thereof immediately (and in any event within 24 hours) and to provide all relevant information about the nature of the incident, the risk that data have been or may be processed unlawfully and the measures that are or will be taken to resolve the incident or limit the consequences/damage as much as possible. The Processor will also specify a point of contact at the Processor who the Controller can contact about this incident. The Processor will take all reasonable steps to mitigate the effects and to minimise any damage resulting from the incident.

7.3 The Processor shall cooperate with the Controller at all times and shall promptly follow the instructions of the Controller, in order to enable the Controller to conduct a thorough investigation into the incident, to formulate a correct response and to take suitable further steps in respect of the incident.

7.4 The term "incident" shall be understood to mean in any case:

a) a complaint or a request (for information) of a natural person with regard to the processing of the Personal Data by the Processor;

b) an investigation into or seizure of the Personal Data by government officials, or any indication that this is about to take place;

c) any unauthorized or accidental access, processing, erasure, loss or any form of unlawful processing of the Personal Data;

d) any breach of the security and/or confidentiality as set out in Article 32 GDPR or Articles 5 and 6 of this Data Processor Agreement, leading to the loss or any form of unlawful processing, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data, or any indication of such breach having taken place or being about to take place.

7.5 In case of an incident as meant in Article 7.4(d), the Data Processor notifies the Data Controller within 24 hours after discovery of the incident. Such notification includes:

i. the nature of the incident;

ii. the date and time upon which the incident took place and was discovered;

iii. the (amount of) data subjects affected by the incident;

iv. which categories of Personal Data were involved with the incident; and

v. whether and, if so, which security measures – such as encryption – were taken to render the Personal Data incomprehensible or inaccessible to anyone without the authorization to access these data. The Data Controller alone may notify any public authority.

7.6 The Processor shall at all times have in place written procedures enabling it to provide an immediate response to the Controller about an incident, and to cooperate effectively with the Controller in addressing the incident, and shall provide the Controller with a copy of such procedures at the request of the Controller.

7.7 All notifications made pursuant to this Article 7 shall be addressed to the employee of the Controller specified in Annex 2 of this Addendum or, if relevant, to another employee of the Controller designated by the Controller in writing during the term of this Data Processor Agreement.

7.8 If this is necessary under applicable law, the Controller shall inform the data subjects, supervisory authorities and other third parties of the incidents. The Processor shall not be allowed to provide information about incidents to data subjects or other third parties, except where the Processor has a legal obligation to do so.

Article 8 Use of Subcontractors

8.1 The Processor shall not subcontract any of its activities as described in the Agreement to any third party (sub-processor) without the prior written consent of the Controller.

8.2 The Processor shall impose the same or stricter obligations on the sub-processor engaged by it as follow from this Data Processor Agreement and the law for itself, and shall monitor compliance thereof by the third party.

8.3 Notwithstanding the consent of the Controller for engaging a third party, the Processor shall remain fully liable towards the Controller for the consequences of subcontracting the activities to a sub-processor. The consent of the Controller for subcontracting activities to a sub-processor shall not affect the requirement of consent in accordance with Article 4.1 of this Data Processor Agreement for the deployment of sub-processors in a country outside the European Economic Area without an adequate level of protection.

Article 9 Liability and Indemnity

9.1 The Processor shall indemnify the Controller and holds the Controller harmless against all claims, actions, third party claims and losses, damage or costs incurred or suffered by the Controller and arising directly or indirectly out of or occurring in connection with a breach of this Addendum by the Processor or sub-processor to meet its obligations and/or any violation by the Processor or sub-

processor of applicable laws in the field of personal data processing in connection with the Annex 1 mentioned in Article 2, including, in any case, the GDPR.

Article 10 Term and termination

10.1 This Addendum enters into force on the date of signature.

10.2 Termination or expiration of this Addendum shall not discharge the Data Processor from its obligations meant to survive the termination or expiration of the Addendum, including e.g. the obligations deriving from Article 5, 6, 9 and 11 of this Addendum.

Article 11 Retention Periods, Return and Destruction of Personal Data

11.1 The Processor shall not retain the Personal Data any longer than is strictly necessary and in any case not longer than until the end of this Data Processor Agreement or, if a retention period has been agreed between the Parties, not longer than this period.

11.2 Upon termination of this Data Processor Agreement, or if applicable at the end of the retention periods agreed, or at the written request of the Controller, the Processor shall either immediately destroy the Personal Data or return them to the Controller, at the discretion of the Controller. At the request of the Controller, the Processor shall provide evidence of the fact that the data have been destroyed or removed. If return, destruction or removal is not possible, the Processor shall immediately notify the Controller thereof. In that case the Processor guarantees that he shall treat the Personal Data confidentially and shall no longer process them.

11.3 Upon the end of the Data Processor Agreement the Processor shall inform all third parties involved in the processing of the Personal Data of the termination of the Data Processor Agreement and shall guarantee that all third parties involved will destroy the Personal Data or assign them to the Controller, at the discretion of the Controller.

11.4 If due to technical limitations a full deletion or destruction of the Personal Data is not deemed possible, the Processor shall take all necessary measures to (i) achieve the closest possible approximation of a full and permanent deletion and/or destruction and (ii) anonymise the remaining Personal Data and render them unavailable for further processing. The Processor shall always inform the Controller in writing.

Article 12 Records

12.1 The Processor will maintain an accurate, up-to-date written log of all processing of Personal Data performed on the Controller's behalf. The written log shall include the following information:

i. the categories of recipients to whom the Personal Data have been or will be disclosed;
ii. to the extent that Personal Data is transferred to a third party outside the European Economic Area, a list of such transfers (including the name of the relevant non- European Economic Area country and organisation), and documentation of the suitable safeguards in place for such transfers; and
iii. a general description of the technical and organisational security measures referred to in this Data Processor Agreement. The Processor will provide the Controller with a copy of such log upon the Controller's request.

Article 13 Final provisions

13.1 All other provisions from the Agreement shall continue to apply without further change. In the event of any contradiction between this Addendum and the Agreement regarding privacy and data protection, this Addendum shall prevail.

13.2 This Addendum shall be subject to Belgian law. Any disputes arising out of or in connection with this Addendum shall exclusively be submitted to the competent courts of Brussels.

Signed at Mechelen on ..... . Each Party confirms to have received one original copy.

Wolters Kluwer	**The Processor**
	Name: Title:

Annex 1 Relevant information pertaining to the Personal Data, the processing purposes and description of the processing activity/activities, security measures and data transfers.

Annex 2 Contact data

ANNEX 1 RELEVANT INFORMATION PERTAINING TO THE PERSONAL DATA, THE PROCESSING PURPOSES AND DESCRIPTION OF THE PROCESSING ACTIVITY/ACTIVITIES, SECURITY MEASURES AND DATA TRANSFERS

1. **Nature of the processing**
   (description of the processing)

2. **Categories of Personal Data being processed**
   Within the framework of this Addendum, the Processor shall solely process following categories of Personal Data:
   (Please list all types of personal data that are begin processed: for example: identification data (name, address, phone, e-mail, date of birth, license plate number, IP-address, …), identification data provided by the government (national ID number, passport number, …), contact data (address, e-mail, IP-address, IMEI, …), social status data (job title, social role, family, …), financial information (bank account, mortgage, loan, investments, payment behavior, rating, …), educational information (diploma, certificates,…), jobrelated data (CV, current and former employers, wages, assessments, …), profile of a person, behavioral data (browser history, payment history, usage history, …), …)

   Special categories of Personal Data:
   (indicate if applicable)

☐ Racial or ethnical origin	☐ Biometric data
☐ Political opinions	☐ Health data
☐ Religious or philosophical beliefs	☐ Data on sex life or sexual orientation
☐ Trade union membership	☐ Criminal convictions and offences and related security measures
☐ Genetic data	

3. **Categories of Data Subjects**
   (indicate of which persons Personal Data are being processed: customers of the Controller, own customers of the Processor, employees of the Processor, employees of the Controller, suppliers, consultants, authors, purchased Personal Data, Personal Data provided by a third party for free, …)

4. **Purpose(s) of the Processing**
   (describe the purpose(s) of the processing)

5. **Retention**
   Personal Data shall be processed and stored during:

6. **Security measures**
   Technical and organisational measures are considered state of the art on the date of signature of this Addendum. The Processor shall evaluate all technical and organizational measures in due time, taking into account the costs of the execution, nature, scope, context and purposes of the processing and the risk involved, taking into account the probability and seriousness of the impact on the rights and freedoms of natural persons.

Detailed technical and organisational measures:	
Access control: buildings	
Access control: systems	
Access control: data	
Pseudonimisation of data	
Encryption of data	
Ensuring the ongoing confidentiality, integrity and availability of the systems and services used by the processing	
Capability to restore the processing and access to its data in a timely manner in the event of a physical or technical incident	
Process for regularly testen, assessing and evaluating the effectiveness of technical and organisational measures	

for ensuring the security of the processing, including penetration testing	
Certification(s)	
Other	

7. **Subprocessors**
Following Subprocessors process Personal Data on behalf of the Processor:

Name	**Address**	**Reason for access to the Personal Data / type of processing**
[...]	[...]	[...]

8. **Transfer of Personal Data**
(indicate if applicable)
All transferred Personal Data shall meet following conditions: *(details on who receives the data (name – address) and copies of documents providing the necessary guarantees, such as the EU model contract clauses, ...)*

☐ no data transfer
☐ transfer to a country within the European Economic Aria (= EU + Iceland + Liechtenstein + Norway)
☐ transfer to a country providing adequate protection (= Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Jersey (UK), Switzerland, Isle of Man, Israel, Japan, New-Zealand and Uruguay)
☐ transfer tot he US under the EU-US Privacy Shield program
☐ transfer under a EU Model Contract
☐ other:

ANNEX 2 CONTACT DATA

Contact person for the Controller:
In the Agreement

Contact data for the Processor:
Name: E-mail: Telephone/Mobile:
Title: