

GENERAL DATA PROTECTION REGULATION ADDENDUM

BETWEEN:

- A. **WOLTERS KLUWER BELGIUM NV**, with its registered office established at Motstraat 30, 2800 Mechelen, Listed in the Antwerp Register of Legal Entities, Mechelen division, and registered for VAT purposes under number BE 0405.772.873,
Hereinafter referred to as “the Processor”

AND:

- B. **The Customer**
And hereinafter referred to as “the Controller”.

The Processor and Controller are hereinafter referred to individually as “the Party” and jointly as “the Parties”.

The Parties have concluded one or more agreements concerning Wolters Kluwer products and/or services (hereinafter referred to as “the Agreement”) and wish by means of this addendum to meet their obligations pursuant to the General Data Protection Regulation 2016/679 of 27 April 2016.

THE FOLLOWING IS AGREED:

Article 1. Definitions

In the framework of this Addendum the following terms have the meanings specified below:

“Applicable Data Protection Law”	: the legislation that affords protection for people’s fundamental rights and freedoms and in particular their right to privacy with regard to the Processing of Personal Data, and that is applicable to the Controller and the Processor; the term “Applicable Data Protection law” also encompasses the GDPR as soon as this enters into force on 25 May 2018;
“Controller”	: the contracting party referred to under point B which, as a natural or legal person, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
“General Data Protection Regulation or GDPR”	: 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, which enters into force on 25 May 2018;
“International Organisation”	: an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries;
“Member State”	: a country that is a member of the European Union;
“Personal Data”	: any information relating to an identified or identifiable natural person (Data Subject);
“Data Subject”	: an identifiable person who can be directly or indirectly identified, in particular on the basis of an identifier such as a name, an identification number, location data, an online identifier or on the basis of one or more

elements characteristic of that natural person's physical, physiological, genetic, psychological, economic, cultural or social identity;

- "Personal data breach"** : breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
- "Processing"** : any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- "Processor"** : the contracting party referred to under point A which processes Personal Data on behalf of the Controller;
- "Services"** : the services provided by the Processor to the Controller and described below in the Annex to this Addendum;
- "Special Categories of Data"** : data relating to race or ethnic origin, political views, religious or philosophical beliefs, trade union membership; genetic data, biometric data processed with the sole aim of identifying a natural person; data relating to health, sexual behaviour or sexual orientation, or judicial data and related security measures;
- "Sub-processor"** : a data processor whose services are enlisted by the Processor and who declares himself/itself to be prepared to receive Personal Data from the Processor that are solely intended for Processing Activities having to be carried out on behalf of the Controller in accordance with the latter's instructions, the terms and conditions of this Addendum and the terms and conditions of a written sub-processing agreement;
- "Supervisory authority"** : an independent public authority established by a Member State pursuant to Article 51 of the GDPR;
- "Technical and Organisational Security Measures"** : the measures aimed at protection of Personal Data against unintentional destruction or unintentional loss, alteration, unauthorised disclosure or access, particularly where the Processing involves the transmission of data via a network, and against all other unlawful forms of Processing;
- "Third Country"** : a country, or a territory or one or more specified sectors within that country, for which the European Commission has not decided that an adequate level of protection is ensured.

Article 2. Details of the Processing

- 2.1 The details of the Processing Activities performed by the Processor on behalf of the Controller as a data processor that has been given the instruction to that end (such as the subject of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects) are given in the Annex to this Addendum, and more particularly the relevant product data sheet(s). The product data sheets of all products and/or services for which the Controller has concluded an Agreement are applicable under this Addendum.
- 2.2 The product data sheet(s), which describe in detail all relevant information on the Processing of Personal Data per Agreement with the Controller, may only be adapted provided the Controller is given prior written notification. Without prejudice to Article 5.2 of this Addendum, modified product data sheets will take effect and be deemed to be binding between the Parties if no written reasoned reaction to this is forthcoming from the Controller within 14 calendar days of receipt of the written notification.
- 2.3 Ownership of the Personal Data shall never pass to the Processor, unless the latter's own Personal Data or those of its employees or agents are concerned.

Article 3. Rights and obligations of the Controller

The Controller remains the responsible data controller for the Processing of Personal Data in accordance with the instructions given to the Processor on the basis of the Agreement, this Addendum and any other instructions. The Controller has ordered the Processor, and will continue to order the Processor for the duration of the data processing for which the order is given, to process the Personal Data solely on behalf of the Controller and in accordance with the Applicable Data Protection Law, the Agreement, this Addendum and the Controller's instructions. The Controller is entitled and obliged to give the Processor instructions regarding the Processing of Personal Data, both in general and in individual cases. Instructions may also relate to the rectification, erasure, portability and blocking of Personal Data. Instructions are generally given in writing, unless urgency or other specific circumstances call for a different form (e.g. orally or by electronic means). Instructions not given in writing must be confirmed in writing immediately by the Controller. Assuming fulfilment of an instruction occasions costs for the Processor, the latter shall first inform the Controller of these costs. The Processor shall only proceed to carry out an instruction once the Controller has confirmed that it will bear the costs associated with fulfilment of that instruction.

Article 4. Obligations incumbent upon the Processor

The Processor shall:

- (a) only process Personal Data in accordance with the Controller's instructions and on the Controller's behalf; these instructions are given in the Agreement, this Addendum and otherwise in documented form as stated in Article 3 above. This obligation to follow the Controller's instructions also applies to the transfer of Personal Data to a Third Country or an International Organisation;
- (b) immediately inform the Controller if the Processor is for any reason unable to carry out an instruction it has been given by the Controller;
- (c) ensure that persons authorised by the Processor to process Personal Data on behalf of the Controller promise to endeavour to keep these data secret or are bound by a suitable duty of confidentiality and that persons having access to the Personal Data shall only process these in accordance with the Controller's instructions;
- (d) implement Technical and Organisational Security Measures that meet the requirements of the Applicable Data Protection Law as specified in greater detail in the Annex before processing the Personal Data and see to it that it provides the Controller with adequate guarantees as regards these Technical and Organisational Security Measures;
- (e) assist the Controller by means of suitable Technical and Organisational Measures, as far as are practicable, with a view to fulfilment of the Controller's obligation to comply with requests for the exercise of Data Subjects' rights concerning information, access, rectification and erasure, restriction of processing, notification, data portability, objection to direct marketing, profiling in the context of direct marketing and automated individual decision-making. Insofar as these practicable Technical and Organisational Measures call for improvements or alterations to the Technical and Organisational Measures referred to in the Annex, the Processor shall notify the Controller of the costs of implementing these additional or altered Technical and Organisational Measures. As soon as the Controller has confirmed that it will bear these costs, the Processor shall go ahead and take these additional or altered Technical and Organisational Measures in order to assist the Controller in complying with requests made by Data Subjects;
- (f) make available to the Controller all the information needed to demonstrate that the obligations mentioned in this Addendum and in Article 28 of the GDPR are being complied with, and enable and contribute to monitoring, including inspections by the Controller or another inspector authorised to this end by the Controller. The Controller is aware that inspections carried out in person and on site may substantially disrupt the Processor's business activities and may cost a lot of time and money. Therefore the Controller may only carry out a check in person and on site if the Controller reimburses the Processor for the costs or expenses the latter incurs as a result of the disruption to its business

activities and if the time and place of the inspection are fixed in advance by mutual agreement between the Parties;

- (g) notify the Controller without undue delay:
- (i) of any legally binding request for disclosure of Personal Data by a law enforcement body, unless this notification is otherwise prohibited, such as for example a prohibition under criminal law aimed at preserving the confidentiality of a law enforcement investigation;
 - (ii) of complaints and requests received directly from Data Subjects (for example complaints and requests relating to access, rectification and erasure, restriction of processing, notification, data portability, objection to direct marketing, profiling in the context of direct marketing and automated individual decision-making) without complying with that request, unless it is otherwise authorised or obliged to do so;
 - (iii) if, on the basis of EU legislation or Member State legislation applicable to it, the Processor is obliged to process Personal Data outside the framework of the Controller's assignment, before going ahead with this processing outside that framework, unless that EU legislation or Member State legislation prohibits this information for significant reasons of public interest; this notification should mention the legal requirement by virtue of that EU legislation or the Member State legislation;
 - (iv) if, in the Processor's opinion, an instruction is in contravention of the Applicable Data Protection Law or other legislation applicable to the Processor; when giving this notification the Processor is not obliged to follow the instruction, unless and until the Controller has confirmed or altered it; and
 - (v) as soon as the Processor becomes aware of a Personal Data Breach at its premises, within 24 hours at the latest. In the event of such a Personal Data Breach the Processor shall assist the Controller, upon the latter's written request, in the Controller's obligation pursuant to the Applicable Data Protection Law to inform the Data Subjects or the Supervisory Authorities, and to document the Personal Data Breach. Contact data relating to the reporting are recorded in the customer service system;
- (h) assist the Controller in a Data Protection Impact Assessment as required on the basis of Article 35 of the GDPR, relating to the Services rendered by the Processor to the Controller and the Personal Data processed by the Processor on the Controller's behalf;
- (i) deal with all questions put to it by the Controller concerning its Processing of the Personal Data to be processed (for example by enabling the Controller to react in good time to complaints or requests made by Data Subjects) and go along with the Supervisory Authority's advice concerning Processing of the transferred data;
- (j) promptly rectify, erase and/or block Personal Data processed on the basis of this Addendum, where it is obliged and requested to do so. If and insofar as Personal Data cannot be erased on the grounds of legal requirements relating to the keeping of data, the Processor should, instead of erasing the Personal Data in question, restrict the continued processing and/or use of Personal Data or remove the corresponding identity from them (referred to hereinafter as "blocking"). If a blocking obligation of this kind is applicable to the Processor, the latter should erase the Personal Data in question at the latest on the last day of the calendar year in which the retention period comes to an end.

Article 5. Sub-processing and transfer of Personal Data

- 5.1 The Controller gives permission for the use of one or more Sub-processors whose services are enlisted by the Processor for provision of the Services and who are mentioned in the product data sheet (see Annex).
- 5.2 If the Processor is planning to bring in new or additional Sub-processors, it should inform the Controller beforehand of any planned changes involving the addition or replacement of any Sub-

processor (“**Sub-processor Notification**”). If the Controller has reasonable grounds for objecting to the use of new or additional Sub-processors, it should immediately notify the Processor of this in writing within 14 days of receipt of the Sub-processor Notification. Should the Controller object to a new or additional Sub-processor and this objection is not unreasonable, the Processor will make reasonable efforts to make changes in the Services available to the Controller or to recommend a commercially reasonable alteration in the Controller’s configuration or the Controller’s use of the Services in order to avoid Personal Data being processed by the new or different Sub-processor to whom/which an objection has been made, without thereby placing an unreasonable burden on the Controller. If the Processor is unable to make this alteration available within a reasonable period, namely not exceeding sixty (60) days, the Controller may terminate the part of the Agreement affected, albeit solely in respect of those Services that cannot be provided by the Processor without the use of the new or different Sub-processor against whom/which an objection has been made by means of a written notification sent to the Processor.

- 5.3 The Processor contractually lays down the same data protection obligation as that stated in this Addendum on all Sub-processors. In particular, the agreement between Processor and Sub-processor provides adequate guarantees for implementation of the Technical and Organisational Security Measures as referred to in the Annex, insofar as these Technical and Organisational Security Measures are important for the services provided by the Sub-processor.
- 5.4 The Processor shall choose the Sub-processor with the necessary care.
- 5.5 If such a Sub-processor is located in a Third Country, the Processor shall, at the Controller’s written request, enter into an EU model contract (Controller > Processor) on the Controller’s behalf (in the Controller’s name), pursuant to Commission Decision 2010/87/EU or take other equivalent measures for the protection of Personal Data. In this case the Controller instructs and authorises the Processor to give Sub-processors instructions on the Controller’s behalf and to make use of all the Controller’s rights vis-à-vis the Sub-processors on the basis of the EU model contract or the other measures taken.
- 5.6 The Processor remains liable vis-à-vis the Controller for fulfilment of the Sub-processor’s obligations should the Sub-processor fail to meet its obligations. However, the Processor is not liable for loss and claims arising from instructions that the Controller has given Sub-processors.
- 5.7 The Annex contains a list of Personal Data transfers for which the Controller gives its permission at the time this Addendum was finalised.

Article 6. Limitation of liability

Any liability arising from or associated with this Addendum is in keeping with, and is solely governed by, the liability provisions set forth in or otherwise applicable to the Agreement. Therefore, and for the calculation of limits of liability and/or determination of applicability of other limitations of liability, any liability arising by virtue of this Addendum shall be deemed to arise by virtue of the Agreement in question.

The Article 7. Term and termination

- 7.1 The term of this Addendum is the same as that of the Agreement in question. Barring any provision to the contrary in this Addendum, rights and obligations in the field of termination are the same as the rights and obligations contained in the Agreement in question.
- 7.2 Once provision of the Services has come to an end the Processor should either erase all Personal Data or return them to the Controller, as the Controller decides, and erase all existing copies unless it is obliged to keep these Personal Data on the grounds of EU legislation or Member State legislation.

Article 8. Miscellaneous

- 8.1 The other terms and conditions of the Agreement continue to apply in unaltered form. In the event of any discrepancy between this Addendum and the Agreement as regards privacy and data protection, the provisions of this Addendum shall take precedence.

- 8.2 The invalidity or unenforceability of any provision of this Addendum shall not have any effect on the validity or enforceability of the other provisions of this Addendum. The invalid or unenforceable provision will be (i) modified in such a way as to guarantee its validity or enforceability and at the same time to ensure that the Parties' intentions are maintained to as great a degree as possible, or - if this is not possible - (ii) construed as if the invalid or unenforceable section in it had never been included. The above also applies if this Addendum were to contain an omission.
- 8.3 This Addendum is governed by Belgian law. Any disputes arising from or relating to this Addendum shall be brought solely before the competent court in Brussels.

ANNEX PRODUCT DATA SHEET(S) WITH RELEVANT INFORMATION CONCERNING PERSONAL DATA, PURPOSES AND DESCRIPTION OF PROCESSING ACTIVITY/ACTIVITIES, SECURITY MEASURES AND TRANSFERS

All information on processing of personal data by the Processor, under the Controller's authority in the context of use of the above-mentioned product, for which the Parties concluded an Agreement, can be found at: <https://www.wolterskluwer.com/nl-be/know/gdpr/product-fiches>