Wolters Kluwer Data Processing Agreement

Both Parties, as identified in the License and Services Agreement Legisway Essentials as signed by (Company name) on the (date) (hereinafter: "Service Agreement")

(More specific between:

1. ***Wolters Kluwer Nederland B.V.**, a company incorporated under the laws of Netherlands, having its registered office at Staverenstraat 15, 7418 CJ in Deventer and registered in the trade register of the Chamber of Commerce under number KvK 38013226 ("Processor" or "Wolters Kluwer"); and*
2. ***(Company name)**, a company incorporated under the laws of Netherlands, having its registered office at (street name, postal code, city) ("Controller" or "Buyer")*

declare to have agreed as follows:

PREAMBLE

WHEREAS, Parties have entered into an agreement (License Agreement) where Processor is responsible for the provision of the cloud-based platform called Legisway Essentials, offering a database for storing and managing of legal documents, including contracts management and corporate housekeeping. Based on this License Agreement, Processor will obtain personal data from Controller which will be processed for the performance of this License Agreement.

NOW, THEREFORE, and in order to enable the Parties to carry out their relationship in a manner that is compliant with law, the Parties have entered into this Data Processing Agreement ("**DPA**") as follows:

1. Definitions

For the purposes of this DPA:

"**Applicable Data Protection Law**"	shall mean the General Data Protection Regulation (EU) 2016/679 and additional rules and implementations of such EU data protection legislation laid down in Dutch national laws and regulations;
"**Controller**"	shall mean the Buyer, as defined under Article 1.1 of Annex 1, who determines as a natural or legal person alone or jointly with others the purposes and means of the Processing of Personal Data;
"**General Data Protection Regulation**" or "**GDPR**"	shall mean 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 which will come into effect on May 25, 2018;
"**International Organization**"	shall mean an organization 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**"	shall mean a country belonging to the European Union;
"**Personal Data**	shall mean any information relating to an identified or identifiable natural person (Data Subject);
"**Data Subject**"	shall mean an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
"**License Agreement**"	shall mean the License and Services Agreement (defined as License Agreement in Article 1, Annex 1) concluded between the Controller and the Processor setting out the terms and conditions for the provision of the Services;
"**Personal Data Breach**"	shall mean a breach of security leading to the accidental or unlawful destruction, loss alteration, unauthorized disclosure or, or access to, Personal Data transmitted, stored or otherwise Processed;

"**Process/Processing**"	shall mean 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"**Processor**"	shall mean Wolters Kluwer Nederland B.V. who Processes Personal Data on behalf of the Controller;
"Services"	shall mean the services provided by the Processor to the Controller and described under 'subject-matter of the processing' in Appendix 1 of this DPA;
"**Special Categories of Data**"	shall mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership; genetic data, biometric data Processed for the purpose of uniquely identifying a natural person; data concerning health or data concerning a natural person's sex life or sexual orientation;
"**Sub-processor**"	shall mean any data processor engaged by the Processor who agrees to receive from the Processor Personal Data exclusively intended for Processing activities to be carried out on behalf of the Controller in accordance with its instructions, the terms of this DPA and the terms of a written subcontract;
"**Supervisory Authority**"	shall mean an independent public authority which is established by a Member State pursuant to Article 51 of the GDPR;
"**Technical and Organizational Security Measures**"	shall mean those measures aimed at protecting Personal Data against accidental destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the Processing involves the transmission of data over a network, and against all other unlawful forms of Processing;
"**Third Country**"	shall mean a country where the European Commission has **not** decided that the country, a territory or one or more specified sectors within that country, ensures an adequate level of protection.

2. Details of the Processing

The details of the Processing operation provided by the Processor to the Controller as a commissioned data processor (e.g., the subject-matter of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects) are specified in Appendix 1 to this DPA.

3. Rights and Obligations of Controller

The Controller remains the responsible data controller for the Processing of the Personal Data as instructed to the Processor based on the License Agreement, this DPA and as otherwise instructed. The Controller has instructed and throughout the duration of the commissioned data processing will instruct the Processor to Process the Personal Data only on Controller's behalf and in accordance with the Applicable Data Protection Law, the License Agreement, this DPA and Controller's instructions. The Controller is entitled and obliged to instruct the Processor in connection with the Processing of the Personal Data, generally or in the individual case. Instructions may also relate to the correction, deletion, blocking of the Personal Data. Instructions shall generally be given in writing, unless the urgency or other specific circumstances require another (e.g., oral, electronic) form. Instructions in another form than in writing shall be confirmed by the Controller in writing without delay. To the extent that the implementation of an instruction results in costs for the Processor, the Processor will first inform the Controller about such costs. Only after the Controller's confirmation to bear such costs for the implementation of an instruction, the Processor is required to implement such instruction.

4. Obligations of Processor

The Processor shall:

(a) process the Personal Data only as instructed by the Controller and on the Controller's behalf; such instruction is provided in the License Agreement, this DPA and otherwise in documented form as specified in clause 3 above. Such obligation to follow the Controller's instruction also applies to the transfer of the Personal Data to a Third Country or an International Organization.

(b) inform the Controller promptly if the Processor cannot comply with any instructions from the Controller for whatever reasons.

(c) ensure that persons authorized by the Processor to Process the Personal Data on behalf of the Controller have committed themselves to confidentiality or are under an appropriate obligation of confidentiality and that such persons that have access to the Personal Data Process such Personal Data in compliance with the Controller's instructions.

(d) implement the Technical and Organizational Security Measures which will meet the requirements of the Applicable Data Protection Law as further specified in Appendix 1 before Processing of the Personal Data and ensure to provide sufficient guarantees to the Controller on such Technical and Organizational Security Measures.

(e) assist the Controller by appropriate Technical and Organizational Measures, insofar as this is feasible, for the fulfillment of the Controller's obligation to respond to requests for exercising the Data Subjects rights concerning information, access, rectification and erasure, restriction of processing, notification, data portability, objection and automated decision-making; to the extent such feasible Technical and Organizational Measures require changes or amendments to the Technical and Organizational Measures specified in Appendix 1, the Processor will advise the Controller on the costs to implement such additional or amended Technical and Organizational Measures. Once the Controller has confirmed to bear such costs, the Processor will implement such additional or amended Technical and Organizational Measures to assist the Controller to respond to Data Subject's requests.

(f) make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and in Art. 28 GDPR and allow for and contribute to audits, including inspections conducted by the Controller or another auditor mandated by Controller. The Controller is aware that any in-person on-site audits may significantly disturb the Processor's business operations and may entail high expenditure in terms of cost and time. Hence, the Controller may only carry out an in-person on-site audit if the Controller reimburses the Processor for any costs and expenditures incurred by the Controller due to the business operation disturbance. The Specific terms under which an audit may take place in relation to Legisway Essentials are stipulated in Appendix 1.

(g) notify the Controller without undue delay:

(i) 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;
(ii) about any complaints and requests received directly from the Data Subjects (e.g., regarding access, rectification, erasure, restriction of processing, data portability, objection to processing of data, automated decision-making) without responding to that request, unless it has been otherwise authorized to do so;
(iii) if the Processor is required pursuant to EU or Member State law to which the Processor is subject to process the Personal Data beyond the instructions from the Controller, before carrying out such processing beyond the instruction, unless that EU or Member State law prohibits such information on important grounds of public interest; such notification shall specify the legal requirement under such EU or Member State law;
(iv) if, in the Processor's opinion, an instruction infringes the Applicable Data Protection Law; upon providing such notification, the Processor shall not be obliged to follow the instruction, unless and until the Controller has confirmed or changed it; and
(v) after the Processor becomes aware of a Personal Data Breach at the Processor. In case of such a Personal Data Breach, the Processor upon the Controller's written request will assist the Controller with the Controller's obligation under Applicable Data Protection Law to inform the Data Subjects and the Supervisory Authorities, as applicable, and to document the Personal Data Breach.

(h) assist the Controller with any Data Protection Impact Assessment as required by Art. 35 of the GDPR and/or any prior consultation as required by Article 36 GDPR that relates to the Services provided by the Processor to the Controller and the Personal Data processed by the Processor on behalf of the Controller.

(i) assist the Controller in dealing with inquiries from Data Subjects (e.g., to enable the Controller to respond to complaints or requests from Data Subjects under Chapter 3 of the GDPR in a timely manner) and abide by the advice of the Supervisory Authority with regard to the Processing of the data transferred.

(j) On request of the Controller correct, erase and/or block Personal Data Processed under this DPA, to the extent that the Processor is required to do so under the GDPR. If and to the extent that Personal Data cannot be erased due to statutory retention requirements, the Processor shall, in lieu of erasing the relevant Personal Data, be obliged to restrict the further Processing and/or use of such Personal Data, or remove the associated identity from the Personal Data (hereinafter referred to as "blocking"). If the Processor is subject to such a blocking obligation, the Processor shall erase the relevant Personal Data before or on the last day of the calendar year during which the retention term ends.

5. Sub-processing

(a) The Controller authorizes the use of Sub-processor(s) engaged by the Processor for the provision of the Services. The Controller approved-Sub-processor(s) will be detailed in Appendix 1.

(b) In case the Processor intends to engage new or additional Sub-processors, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of any Sub-processor ("**Sub-processor Notice**"). If the Controller has a reasonable basis to object to the use of any such new or additional Sub-processor, the Controller shall notify the Processor promptly in writing within 14 days after receipt of the Sub-processor Notice. In the event the Controller objects to a new or additional Sub-processor, and that objection is not unreasonable, the Processor will use reasonable efforts to make available to the Controller a change in the Services or recommend a commercially reasonable change to the Controller's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new or additional Sub-processor without unreasonably burdening the Controller. If the Processor is unable to make available such change within a reasonable period of time, which shall not exceed sixty (60) days, the Controller may terminate the effected part of the License Agreement with respect only to those Services which cannot be provided by the Processor without the use of the objected-to new or additional Sub-processor by providing written notice to the Processor.

(c) The Processor shall impose the same data protection obligation as set out in this DPA on any Sub-processor by contract. The contract between the Processor and the Sub-processor shall in particular provide sufficient guarantees to implement the Technical and Organizational Security Measures as specified in Appendix 1, to the extent such Technical and Organizational Security Measures are relevant for the services provided by the Sub-processor.

(d) The Processor shall choose the Sub-processor diligently.

(e) In case any such Sub-processor is located in a Third Country, the Processor upon the Controller's written request will enter with the relevant Sub-processor on the Controller's behalf (in the name of the Controller) into EU Model Contract (Controller to Processor), pursuant to Decision 2010/87/EU. In this case, the Controller instructs and authorizes the Processor to instruct Sub-processors in the Controller's name and to make use of all Controller's rights vis-a-vis the Sub-processors based on the EU Model Contract.

(f) The Processor shall remain liable to the Controller for the performance of the Sub-processor's obligations, should the Sub-processor fail to fulfill its obligations. However, the Processor shall not be liable for damages and claims that ensue from the Controller's instructions to Sub-processors.

6. Limitation of liability

Any liability arising out of or in connection with this DPA shall follow, and be exclusively governed by, the liability provisions set forth in, or otherwise applicable to, the License Agreement. Therefore, and for the purpose of calculating liability caps and/or determining the application of other limitations on liability, any liability occurring under this DPA shall be deemed to occur under the relevant License Agreement. Furthermore, Parties agree as follows:

i. Each Party shall be fully liable for any fines imposed on it by supervisory authorities that are intended to punish that Party for its violations of the Data Protection Laws.
ii. Each Party that fails to comply with the Applicable Data Protection Law (the "Indemnifying Party") shall indemnify the other Party against any claims from third parties resulting from such failure of the Indemnifying Party. This indemnity is not subject to any limitation of liability clause in the Agreement.

7. Duration and termination

(a) The term of this DPA is identical with the term of the relevant License Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the relevant License Agreement.

(b) The Processor shall, at the choice of the Controller, delete or return all Personal Data to the Controller after the end of the provision of Services, and delete any existing copies unless EU or Member State law requires the Processor to retain such Personal Data.

8. Miscellaneous

(a) In the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, the provisions of this DPA shall prevail with regard to the Parties' data protection obligations. In case of doubt as to whether clauses in such other agreements relate to the Parties' data protection obligations, this DPA shall prevail.

(b) Should any provision of this DPA be invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or – should this not be possible – (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. The foregoing shall also apply if this DPA contains any omission.

(c) This DPA shall be governed by the same law as the License Agreement except to the extent that mandatory Applicable Data Protection Law applies.

On behalf of the Controller:

Name:

Position:

Address:

Date:

Signature:

On behalf of the Processor:

Name:

Position:

Address:

Date:

Signature:

APPENDIX 1 - GDPR PRODUCT SHEET
Legisway Essentials

1. Nature of the Processing

Legisway Essentials is a SaaS software that saves the data via a cloud service, offering a platform-based database for storing and managing legal documents, including and not limited to, contracts management and corporate housekeeping.

2. Categories of Personal Data that are processed

Processor will process the following categories of Personal Data from the Controller exclusively in the context of the License Agreement:

- Identity data (last name, first name, login name)
- Contact information (address, e-mail, IP address, telephone, fax)
- Behavioural data (user history)

In addition, the Processor may process the Personal Data originated by the Controller. The Personal Data originated, entered and uploaded in Legisway Essentials by the Controller will be at the Controller's sole discretion and risk. The Processor will not have access to or be able to be aware of what kind of Personal Data has been originated by the Controller and as such the Processor cannot know in advance what kind of personal data will be originated, entered and uploaded in Legisway Essentials by the Controller. However, within the purpose of the performance of the Services Agreement categories of data originated by the Controller may include the following:

- Identity data (name, address, mobile phone, e-mail, date of birth, ...)
- Identity data issued by the government (national register number, passport number, ...)
- Social status (family situation, ...)
- Financial information (bank account number, ...)

3. Categories of Data Subjects

- Clients and partners of the Controller
- Shareholders, employees and other staff members of the Controller, including trainees, research assistants and unskilled workers;
- Other persons whose data are processed by the Controller, such as counterparties.

4. Purposes of the processing

Processor stipulates that you can use Legisway Essentials for the purposes below:

- Central management of dossiers, contact data and documents
- Linking to your internal and external sources
- Extensive search and reporting possibilities
- Exporting information for reports and so forth

5. Retention period

As the Controller, you determine yourself the retention period of your Controller information (dossiers, identity data, documents, etc.).

Processor makes a backup of all Controller databases daily. This backup is kept for 30 days.

Personal Data will be processed and kept for the following periods:

- After migration of your data from another software package: we keep no information after migration from the former software package. The Controller itself is responsible for copying/backup of this information and making it available to Processor if necessary.
- Personal Data via support/helpdesk: contacts are anonymised six months after the termination of the contract. As Controller you need to make sure not to transmit sensitive data during the ticket resolution (screenshot etc).
- Copy of your data in connection with support/helpdesk: to resolve a technical problem, we move a copy of a specific portion of your data to an encrypted test environment. Data from production to test environment are transported with encrypted backups, and test environment also have both transport and file encryption in place. Your permission is requested in advance for this. This data is only used to resolve the problem that has occurred and will be deleted from the test environment after the procedure.
- After the end of the License Agreement: we provide the Personal Data in a general and accessible file format. Controller can easily extract data, including Personal Data, from Legisway Essentials in the general and accessible file format available in the system (e.g. Excel, Word etc.). Subsequently we keep the data on our servers for four months.

6. Support/helpdesk/consultants

To resolve an issue or carry out additional configuration, Processor needs access to the database of the Controller.

- The Controller can give the Processor's employee access to Legisway Essentials by giving consent for a determinate purpose. For some systems, Controller can give access to Legisway Essentials to Processor's employee by activating the Support Access option in the database. The Controller can switch off this option at all times.
- If access to the technical systems of the Controller is required, Processor will obtain access to the computer of the Controller via PC sharing. Activation by the Controller is required for remote access; this is done by entering a code provided by Processor or by a pop-up requiring your consent. The Controller is responsible for blocking/protecting all confidential information before granting access.

7. Security measures

In accordance with the GDPR regulations, Processor will take appropriate technical and organisational measures, to be assessed on the basis of the state of the art at the time the License Agreement is concluded, and will evaluate these measures over time, taking into account the costs of implementation, nature, scope, context and objectives of processing, and the risk of differences in the degree of probability and seriousness for the rights and freedoms of natural persons.

DETAILED TECHNICAL AND ORGANISATIONAL MEASURES

7.1 Access control: buildings

Access to the buildings of Processor is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.

The Controller must also ensure that adequate security measures and access to their buildings are taken.

7.2 Access control: systems

As Processor, any access to networks, operational systems, user administration and applications requires the necessary authorisations: advanced password procedures, automatic timeout and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.

The Controller must also ensure that adequate security measures for their passwords and other electronic access information are taken.

7.3 Access control: data

As Processor access to data by Processor itself is controlled by organisational measures: user administration and user accounts with specific access, personnel trained with regard to data processing and security, separation of the operational systems and the test environments, allocation of specific rights and maintaining histories of use, access and deletion.

7.4 Data encryption:

7.4.1 Transport

The HTTPS data transmission is encrypted with a 2048-bit PKI certificate and is certified by Norton.

7.4.2 At rest

We are encrypting databases on disks with a specific certificate / private key, using AES algorithm.

7.5 Ability to guarantee ongoing confidentiality, integrity, availability and resilience of processing systems and services

Access control for Personal Data follows the guidelines for internal control, including the policy for access to information of the organisation, implementation of a user administration system and access rights, creation of awareness among employees on dealing with information and their passwords, network access control, including separation of sensitive networks, and control of access to the operating system and underlying applications. Specifically, the measures include:

- written/programmed authorisation structure;
- differentiated access rights (including for reading, modifying, deleting);
- definition of roles;
- logging/auditing.

Personal Data are segregated. The measures include:

- separation of functions (production/test data);
- segregation of highly sensitive data;
- purpose limitation/compartmentalisation;
- policy/measures to ensure separate storage, modification, deletion and transfer of data.

For the Controller, Legisway Essentials requires the user to use a password to access the Legisway Essentials system, which ensures the confidentiality of all data entered in the management system. Legisway Essentials also offers the possibility of managing the user rights to segment the information accessible within the Legisway Essentials system. The Controller is therefore required to establish confidentiality rules within the company.

7.6 Ability to restore the availability of and access to the Personal Data promptly in the event of a physical or technical incident

The availability of data is controlled by means of a permanent network monitoring system. To prevent data loss, a daily data backup with defined retention periods is conducted. Further measures include:

- backup procedures;
- overvoltage protection;
- physically separate storage of backup data carriers;
- mirroring of server hard drives (RAID);
- antivirus systems/SPAM filters/firewall/intrusion detection system/disaster recovery plan;
- fire/water protection systems (including fire extinguishing system, fire doors, smoke/fire detectors).

7.7 Process for regularly testing, assessing and evaluating the efficacy of technical and organisational measures to guarantee the security of the processing:

7.7.1 Monitoring

The Legisway Essentials system is continuously monitored:

- In the framework of the 24/7 monitoring, both the health of the system and the performance of the application carefully monitored for each client individually.
- An independent external business conducts intrusion tests every year.
- Moreover, the intrusion detection system is always active and gives real-time warnings.
- The Legisway Essentials website is also certified.
- McAfee Security carefully monitors Legisway Essentials every day: certifies that the website is secure, resistant to viruses and intrusion attempts, and protected from attacks of hackers on servers and data transmission.
- We are informed of any risks in real time, so that we can block attacks immediately.
- Norton Symantec continuously monitors our encrypted data transmission via the SSL certificate.
- A vulnerability scan takes place monthly and we receive the associated report.

7.7.2 Audits

Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and under Art. 28 GDPR, including the possibility to review audit reports on-site at the designated Processor office. The Controller is aware that any in-person on-site audits may significantly disturb the Processor's business operations and may entail high expenditure in terms of cost and time. Therefore, Parties agree that:

i. Processor enables Controller to review compliance of Processor with this agreement by making available to the Controller as its request any audit reports already in possession of the Processor.

ii. If there is any evidence to suggest that Processor does not comply with its obligations under this Agreement, Controller may, by obtaining the Processor's consent, perform a secondary audit. The costs of a secondary audit will be borne by Controller unless the audit demonstrates any non-compliance by Processor (in which case the Processor will bear the reasonable costs). If the secondary review shows that Processor does not fully comply with its obligations under this Agreement, Processor shall undo and/or repair the shortcomings identified by the review without delay.

8. Sub-processors

The following Sub-processor(s) perform services on behalf of Processor with regard to personal data:

Name of Subprocessor	Activity	Data localization	Sub-sub processor/Activity/Localization
Wolters Kluwer Global Business Services Italia Via dei Missaglia 97, 20142, Milano, Italia	Management of Cloud	Italy	AWS Europe (Amazon EMEA SARL)/ Management of Cloud/Germany AWS Europe (Amazon EMEA SARL)/Hosting, recovery and backup datacenter/Ireland
DELLA AI UK Ltd. 5 Countess Road, NW5 2NS, London, UK	Only for Indexing Service*: Provider of service And support level 2	France	Orange Business service/Hosting/France
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth, Germany	Only for Teamdocs* (option): Provider of the service	Germany	Telekom Deutschland GmbH (Scanplus GmbH)/Hosting/Germany
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth, Germany	Only for Teamdocs* (option) : Support level 2	Germany	Toppan Merrill GmbH /software editor and support level 3/Germany
Claranet SAS 2 Rue Breguet, 75011 Paris, France	Only for Mail to Legisway* (option) : Hosting and datacenter	France	Equinix/Hosting/France Telecity/Hosting /France
Wolters Kluwer Global business services B.V. Zuidpoolsingel 2, 2408 ZE Alphen aan den Rijn, The Netherlands	Only for Word2PDF* (option): Hosting and datacenter	The Netherlands	Microsoft Azure/Hosting/Europe