Wolters Kluwer Data Processing Agreement

Both Parties, as identified in the License and Services Agreement Legisway Enterprise 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 the License and Services Agreement above (hereinafter: "**Agreement**") where Wolters Kluwer is responsible for the provision of Legisway Enterprise and services related thereto. As a result of the activities under the aforementioned Agreement, Wolters Kluwer may process certain personal data on behalf of Buyer.

NOW, THEREFORE, and in order to enable the Parties to carry out their relationship in a manner that is compliant with applicable 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 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;
"**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;
"**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 as stated in the Agreement and Appendix 1 to 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 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 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.

In case specific instructions given by the Controller lead to customized measures (and are not necessary according to the Applicable Data Protection Law) and the implementation of such specific instructions will lead to additional costs for the Processor, the Processor shall inform the Controller about such costs. Only after the Controller's written confirmation to bear these costs for the implementation of such specific instructions and customized measures, the Processor is required to implement such instructions.

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 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 Article 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 Enterprise 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 Data Breach at the Processor. In case of such a 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 Data Breach;

(h) assist the Controller with any Data Protection Impact Assessment as required by Article 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 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 of the transfer of personal data to a Third Country (for example by engaging a Sub-processor in a Third Country), the Processor will inform Controller about this and will make sure that such transfer complies with all obligations under this DPA and the GDPR. In case Processor engages a Sub-processor in a Third Country, Processor shall enter with the relevant Sub-processor into the EU Standard Contractual Clauses (Processor-Processor).

(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 exclusively governed by, the liability provisions set forth in, or otherwise applicable to, the 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 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 Agreement. Save as otherwise agreed herein, termination rights and requirements shall be the same as set forth in the relevant Agreement.

(b) The Processor shall, at the choice of 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 Agreement except to the extent that mandatory Applicable Data Protection Law applies.

APPENDIX 1 TO THE DPA - GDPR PRODUCT SHEET
Legisway Enterprise

1. Nature of the Processing

Legisway Enterprise is software which supports businesses' legal departments with a variety of tasks, including (but not limited to): contract management (storing and managing legal documents), corporate housekeeping, litigation management, claims management and brand & patent management. Legisway Enterprise may be provided by Processor to the Controller based on either an On Premise model or a Webservice (SaaS) model.

a. Webservice: When Legisway Enterprise is provided as an online service, then everything Controller uploads via Legisway Enterprise will be stored on servers/systems of Processor and/or its Sub-Processors. This includes legal documents with names & signatures, personal information of Controller's business contacts, etc. Besides storing such information, Processor will also process certain personal information when providing support to the Controller etc.

b. On Premise: When Legisway Enterprise is provided on an 'On Premise' model, then Legisway Enterprise will be installed on Controller's IT environment. In this case everything Controller uploads via Legisway Enterprise will be stored on servers/systems of the Controller and/or its suppliers. In case of an On Premise model, processing of Personal Data by the Processor may only take place when: the Processor is implementing (an update of) Legisway Enterprise on Controller's systems, the Processor is importing/exporting content of Controller, the Processor is providing support, etc.

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 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 Enterprise 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 Enterprise by the Controller. However, within the purpose of the performance of the Agreement of Personal Data originated by the Controller may include the following:

- Basic identity data. First name, last name and business email address is often the minimum amount of data stored per Data Subject. Further optional information may also be entered where needed as part of a given business process (e.g. business address, business telephone number, job title) whose processing purpose is defined by the Controller.

2. Categories of Data Subjects

Legisway Enterprise gathers, stores, and handles data related to the identification and management of the Client company's contracts and, more generally, data related to businesses' legal department processes. The Personal Data handled in Legisway Enterprise is limited and may include Personal Data from:

- The users using Legisway Enterprise (often employees of Controller);
- Signatories, managers, people from procurement, etc. related to contracts (*Contract module* and *DialogBox module*);
- Any third parties in the litigation information (*Litigation* module)
- Contacts, corporate officers, shareholders and other people connected to a certain company stored in Legisway Enterprise (*Corporate* module)
- Contacts (designers, inventors, etc.) in the brand and patent filing information (*PI* module)
- Contacts, managers, and participants in the site management information (*Site* module)
- Any third parties in the claims information (*Claims* module)

3. Purposes of the processing

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

- Management of a repository for various types of business files depending on the Legisway Enterprise modules that have been purchased by the Controller (Contracts, Litigation, Corporate, …).
- Management of a list of companies (internal or external to the Controller's group) that are used within the managed business files.
- Management of a list of contacts within the managed companies that are used within the managed business files.
- Searching information and generating output (graphical or Excel) from the managed information.

4. Retention period

The Controller is in charge of the Personal Data stored and managed within Legisway Enterprise and defines itself the lifetime of the data. Should the Agreement be terminated, the Parties shall discuss what to do with content of Controller (the data) in Legisway Enterprise. Should Controller decide to end their use of Legisway Enterprise, Processor undertakes, for a maximum cost established in advance, to provide Controller with all their data in a format that can be used immediately (such as Excel or XML). Parties may agree on the return or transfer of the content of Controller to the Controller or a third party appointed by the Controller. If no return or transfer of the content of the Controller is agreed upon, then Processor will retain the content of the Controller for two months after termination of the Agreement and then destroy the content of the Controller.

In the case Controller uses the Webservice (SaaS) the Processor will make daily backups of the content of the Controller. This copy will be kept for four weeks.

Processor may also process the content of the Controller, which may include personal data, when providing support. Personal data (emails etc.) exchanged with Processor's support department will be deleted six months after termination of the Agreement.

In order to solve technical issues identified by the Controller, Processor may be required to copy some of the Controller's data into a test environment for investigation. Such copies are only made with explicit consent of the Controller. Such copy is exclusively used for the purpose of technical issues analysis. These copies are destroyed immediately after the technical issue is solved.

5. Security measures

In accordance with the GDPR regulations, Processor will take appropriate technical and organizational measures, to be assessed on the basis of the state of the art at the time the 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.

6. Detailed technical and organisational measures

a. Access control: buildings

Access to the buildings of Processor is controlled by both technical and organizational measures: access control with personalized badges, locking of doors, reception procedures for visitors. The Controller must also ensure that adequate security measures and access to their buildings are taken.

b. Access control: systems

As Processor, any access to networks, operational systems, user administration and applications requires the necessary authorizations: 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. Several authentication management modes are available depending on the options to which the Controller is subscribed:

- A "simple" authentication using usernames and passwords set/chosen by the users and administrators.
- Authentication via a link to the Controller's LDAP directory.
- Authentication via integration with an SSO (Single Sign-On) solution.
- Access filtering by IP address. (A white list that corresponds to the public IP address of the Controller's internet pathways).
- The physical and logical architecture guarantees that Controller works in an environment that is separate and isolated from other clients.

In the case of simple authentication by username/password, a password policy must be applied by the Controller. This policy covers the following aspects:

- Minimum password length
- Password complexity
- The prohibition of "trivial" passwords
- Regular password expiry

c. Data encryption:

i. In Transport

HTTPS is used when data is transferred from the Controller to Legisway Enterprise.

For the Webservice model and for exchanges related to implementing LDAP or SSO authentication, Processor recommends implementing an encrypted IPSEC tunnel for SAAS deployments. If Controller wishes to implement interfacing between Legisway Enterprise and their own system, Processor also recommends an encrypted IPSEC tunnel for SAAS deployments.

Messages are sent by the platform to notify users of certain events (an approaching deadline, a task, etc.) These emails are not encrypted and contain no critical business information and no content (contract, a related document, etc.)

ii. At rest

As an option, Processor offers to encrypt certain fields of sensitive data in the database. The goal is that, even in the case of an unauthorised distribution of the Client database, this information remains unusable. When this option is implemented, the fields in question are encrypted and decrypted by the application server when they are accessed for reading and writing. The encryption keys are managed by the application server.

d. Ability to guarantee ongoing confidentiality, integrity and availability of processing systems

Access control for Personal Data follows the guidelines for internal control, including the policy for access to information of the organization, 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.
For the Controller, Processor requires the User to use a password to access Legisway Enterprise, which ensures the confidentiality of all data entered in Legisway Enterprise. The Processor also offers the possibility of managing the user rights to segment the information accessible within Legisway Enterprise. The Controller is therefore required to establish confidentiality rules within its company.
Actions on Processor's systems are logged which must ensure an audit trail is available should any incidents occur.
Processor applies the good practices recommended by OWASP (www.owasp.org) when developing the Legisway Enterprise software (and more particularly the "Top 10" project recommendations: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project)

e. Ability to restore the availability of and access to the Personal Data

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;
- antivirus systems/SPAM filters/firewall/intrusion detection system/recovery plan;

f. Process for regularly testing, assessing and evaluating the efficacy of technical and organizational measures to guarantee the security of processing:

i. Monitoring

The Legisway Enterprise system is continuously monitored:

- Processor's hosting partner Claranet constantly monitors security faults and related updates and regularly provides recommendations about security updates to Processor. These security updates are applied regularly based on these recommendations.
- An independent external business conducts intrusion tests every year.
- Moreover, an intrusion detection system is always active and gives real-time warnings.

- A vulnerability scan is performed regularly.

ii. Audits

Processor will make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in this DPA and under Article 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:

a. 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.

b. 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.

7. Backups, test environment & sub-processors

7.1 Elements specific to an on-premise model

For an on-premise model, the essential processes related to usage and security are borne by the Controller.

- *Backups and restorations*

Legisway recommends daily backups, but the implementation and verification of backups is the responsibility of Controller.

- *Test environment*

Processor recommends that Controller have at least two environments on their platform, with one production environment and a test/approval environment.

- *Sub-processor(s)*

In the on-premise model Processor does not make use of sub-processors in the use phase.

7.2 Elements specific to the Webservice model

- *Backups*

Daily backups are being made of the content in the Webservice by Processor. Such backups will be deleted after 4 weeks.

- *Test environment*

If agreed upon by both Parties, Controller may have access to two environments, including one production environment and one test/approval environment.

- *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
VP&White SAS 62 bis avenue André-Morizet, 92100 Boulogne-Billancourt, France	Configuration	France	--
S. Blavet	Configuration	France	--
Pharmadvize SARL 37 rue d'Amsterdam 75008 Paris, France	Training	France	--
Freelancer trainers	Training	France	--
Claranet SAS 2 Rue Breguet, 75011 Paris, France	Hosting and datacenter for Cloud ENTERPRISE	France	Equinix/hosting/France Telecity/hosting /France Telehouse/hosting/France
Claranet SAS 2 Rue Breguet, 75011 Paris, France	Only for Mail to Legisway* (option) : Hosting and datacenter	France	Equinix/hosting/France Telecity/hosting /France
DELLA AI UK Ltd.	Only for Indexing Service*: Provider of service and support level 2	France	Orange Business service/ hosting/France

at 5 Countess Road, NW5 2NS, London, UK			
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
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
Wolters Kluwer Legal Software France SAS 11 avenue Michel Ricard, 92770 Bois-Colombes, France	Third level of support, consulting and software development	France	--