SCHEDULE 2BIS: DESCRIPTION OF PERSONAL DATA PROCESSING

Software Services: LEGISWAY

This Schedule "Description of Personal Data Processing" is attached to the Data Processing Addendum (DPA) that is subject to and made part of the Agreement between Customer (Controller) and Provider (Processor) named on the Agreement and applies solely to Legisway. This Schedule may be updated from time to time by Provider as new versions of the Software Services are available as part of the Maintenance Services provided to Customer in accordance with the Agreement and as described in the Schedule "Maintenance Services and Service Level Agreement". The updated terms of this Schedule apply between the Parties as of the date of availability of the new version of the Software Services.

1. Processing of Personal Data

A. Purposes of the Processing

Provider, as Processor, may, on behalf of Customer and following Customer's instructions, process Customer's Personal Data in the course of execution of the Agreement to provide Software Services and/or Professional Services including where applicable for:

- Installation
- Data migration, implementation, configuration and testing
- Hosting, storage, and supervision
- Backup and disaster recovery

Maintenance Services as Data Controller, Customer shall ensure that no Personal Data are transmitted to Processor when reporting an Error to Provider's support services (in the form of screenshots, etc.).

Customer, as Data Controller, is responsible for defining the purposes of the Processing it performs using LEGISWAY.

B. Types of Personal Data that are processed

As Data Controller, Customer may input Customer Data including Personal Data in LEGISWAY or otherwise provide Customer Personal Data in connection with its subscription to Legisway, the extent of which is determined and controlled by Customer in its sole discretion but which may include in its standard configuration, the following basic categories of Personal Data:

- First and last names of natural persons
- Titles
- Contact information (including home and work street and email addresses, telephone numbers, IP address)
- Professional life data, etc.

Legisway may contain free-text fields or comment fields.

C. Categories of Data Subjects

As Data Controller, Customer may input Customer Data including Personal Data in LEGISWAY or otherwise provide Customer Personal Data in connection with its subscription to Legisway, the extent of which is determined and controlled by Customer in its sole discretion but which may include information with respect to the following categories of data subjects: employees, independent contractors, officers, directors, advisors, parties and counter-parties to contracts, claimants, and vendors.

D. Nature of Processing

The nature of Processing depends on the services provided by Processor under the Agreement and may include recording, organization, modification, extraction, consultation, disclosure by transmission, storage, limitation, erasure or destruction.

E. Retention period

Provider as Data Processor, will process Customer Personal Data for the period of time appropriate for the performance of the Agreement. Provider shall store Customer Data and shall make backups during the term of the Agreement in accordance with the provisions of the Agreement. Provider shall keep Customer Data, including, if applicable, Personal Data in the following cases and for the following retention periods (subject to legal obligations or statutory limitation periods):

- Copy of Customer Data (DUMP) to support: To solve a technical problem, Provider may need to obtain or copy part of Customer Data including, if applicable, Personal Data to a test environment after having requested Customer's consent. Such Customer Data is only used to solve the problem being addressed and is deleted from the test environment at a maximum of two (2) months after the incident is handled;

- After Data migration: Provider shall keep the migrated data for a period of two (2) months in order to finalize the corrections during this period, if necessary. Customer is responsible for copying/backing up the Data and making it available to Provider after this period as necessary;

- After termination/expiration of the Agreement: As part of the reversibility services provided for in the Agreement, if any, Customer Data shall be returned to Customer in the agreed format. Provider shall then retain the corresponding databases for four (4) months (or such other period as specified in the Agreement) on its servers before complete destruction ;

As Data Controller, Customer shall determine the retention period for Personal Data managed by/in LEGISWAY.

2. Technical and Organizational Measures

Taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the Processing, as well as the risks for the rights and freedoms of Data Subjects, Provider and Customer shall take the appropriate Technical and Organizational Security Measures ("TOMs") to ensure a level of security appropriate to the risk. TOMs implemented by Provider are at a minimum as follows:

A. Access control: Provider's Buildings

Access to the buildings of Provider is controlled by both technical and organizational measures: access control with personalized badges, locking of doors, and reception procedures for visitors.

B. Access control: Systems

Access to Provider networks, operating systems, user administration and applications require the required authorizations: advanced password procedures, automatic timeout and blocking in case of wrong password, individual accounts with history, access review, encryption, hardware and software firewalls.

C. Access control: Data

Provider implements the following measures: user administration and user accounts with specific access, personnel trained in data processing and security, partitioning between operating systems and test environments, granting of specific rights and keeping of usage, access and deletion logs.

D. Data encryption and protection of exchanges

Encryption at rest and in transit are available to protect data against unauthorized access and maintain data integrity.
The HTTPS data transmission between LEGISWAY servers and the Customer is encrypted with the TLS 1.3 protocol.

E. Means to ensure the confidentiality, integrity, availability, and ongoing resilience of processing systems and services

Access control to Personal Data is in compliance with internal control guidelines, including Wolters Kluwer's information access policy, the implementation of user administration system and access rights, raising awareness of employees in the management of information and their passwords, the control of network access and underlying applications. Measures consist of:

- in a written/programmed authorization structure;

- in differentiated access rights, e.g., to read, modify or delete data;
- in a definition of roles;
- in an activity and audit log

Personal Data is partitioned. Measures include:

- Separating functions (production/test data);
- Limiting purposes of processing; compartmentalization
- Rules/measures to ensure separate storage, modification, deletion and transfer of data.

LEGISWAY requires the User to use a password to access LEGISWAY, which ensures the confidentiality of all data entered in the system. LEGISWAY also offers the possibility of managing the User rights to segment the information accessible within LEGISWAY. Customer is therefore required to establish confidentiality rules within their organization.

F. 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 data backup with defined retention periods is made. Further measures include:

- backup procedures;
- overvoltage protection;
- physically separating storage of backup data carriers;
- mirroring of server hard drives (RAID);
- Endpoint detection and response/SPAM filters/firewall/intrusion detection system/disaster recovery plan/Business Continuity Plan;
- fire/water protection systems (including fire extinguishing system, fire doors, smoke/fire detectors);
- procedure to manage security incident: Provider implements security incident management processes with notifications of Data Breach in accordance with the Data Processing Addendum.

G. Process for regularly testing, assessing, and evaluating the efficiency of technical and organizational measures to guarantee the security of the processing

LEGISWAY is monitored continuously:

- Health and performance monitoring is conducted in all computing systems
- Provider conducts internal and external vulnerability and penetration testing of Legisway and the infrastructure on a periodic basis.

In addition, the intrusion detection system is always active and issues alerts in real time.

H. Hosting

LEGISWAY is hosted in Germany on AWS Europe datacenters and in Ireland (back up)

3. Subprocessors

Customer accepts that Provider, as Processor, may engage Sub-processors to carry out specific data processing activities (including the management of cloud services, hosting services, Maintenance Services, etc.) on behalf of Customer:

- Provider Affiliates identified in the intra-group transfer agreement in place within the Wolters Kluwer group include the following:

Provider Affiliate	Data Localization
Wolters Kluwer Legal Software France SAS (except when acts as the Data Processor)	France
Wolters Kluwer Italia S.R.L	Italy
Wolters Kluwer Global Business Services B.V.	The Netherlands
Wolters Kluwer Technology B.V.	The Netherlands

- Third party Sub-processors

Third party Sub-processor	Activity/data localization
ABBYY Europe Landsberger Str. 300 80687 Munich, Germany	OCR: Provider of service and support level 2/Ireland (on MS Azure)
Keynit SAS, 121 rue d'Aguesseau, 92100 Boulogne Billancourt, France	Hosting (Project Phase France)
Claranet SAS, 2 rue Breguet, 75011 Paris, France	Hosting and data center management for Mail to Legisway/France
Teleperformance Portugal Edificio Marconi, Av. Alvaro Pais 2, 1600-873 Lisbon, Portugal	Support Level 1 & level 2/Portugal
VP&White SAS, 62 bis avenue André-Morizet, 92100 Boulogne Billancourt, France	Professional Services/France, UK
NEA IDF SAS 41 rue de Bayern, 75017 Paris, France	Professional Services/France