SCHEDULE 2BIS : LEGISWAY ENTERPRISE GDPR PRODUCT SHEET AND TECHNICAL AND ORGANIZATIONAL MEASURES

Provider, as Processor, may process Personal Data of Customer in the course of execution of the Agreement to provide Software Services and/or Professional Services, and for example to perform the following services :

- Installation and configuration of LEGISWAY ENTERPRISE
- Hosting and supervision of LEGISWAY ENTERPRISE
- Data migration
- Support and Maintenance
- User trainings

The provisions of the Data Processing Agreement ("DPA") shall apply between Provider and Customer in this respect and are supplemented by the following terms and conditions.

PROCESSING OF PERSONAL DATA

A. Categories pf 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)
- Users IP address (audit trail)

As Data Controller, Customer may enter, store and manipulate in LEGISWAY ENTERPRISE Customer Data related to the identification and management of contracts and more broadly Customer Data related to the processes of the Legal Departments of companies including Personal Data.

In its standard configuration, LEGISWAY ENTERPRISE offers basic fields that can be filled in by Customer and manipulate Personal Data such as name, address, phone number, e-mail address, date of birth, ...

Additional optional information may also be entered when necessary in the context of a given business process (business address, business telephone) according to the processing purpose defined by Customer. The presence of such fields is the result of a deliberate choice on the part of Customer during the project phase (settings requested by the Customer to the Provider) or during the administration of the Software (configuration/setting performed by Customer or a third party on behalf of Customer) and thereby under its exclusive liability).

In the standard configuration of LEGISWAY ENTERPRISE, no free text comment fields in the directory of natural persons. The presence of any such field is the result of a deliberate choice on the part of the Customer in the project phase (setting/configuration requested by Customer to the Provider) or during the administration of the Software (configuration/setting performed by Customer or a third party on behalf of Customer) and thereby under its exclusive liability.

Personal data is entered by Users via the Software features for the purposes described herein. Personal Data are not directly collected from the Data subject themselves. The Personal Data originated, entered and uploaded in LEGISWAY ENTERPRISE by Controller will be at the Controller's sole discretion and risk.

The subprocessor hosting LEGISWAY ENTERPRISE Cloud is not approved to host health data. Consequently, the Provider recommends that Customer limit the configuration of LEGISWAY ENTERPRISE related to health data in this context.

B. Categories of Data Subjects

LEGISWAY ENTERPRISE may process Personal Data from the following Data Subjects:

- 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)

C. Purpose of Processing

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

LEGISWAY ENTERPRISE may be used for the following purposes :

- 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.

No interconnection with other systems is required as standard for LEGISWAY ENTERPRISE to function properly, and, in particular, no information will be exported to other systems from the directory of natural persons.

Note: interconnections are sometimes implemented at the request of the Customer. These interconnections are then carried out under Customer supervision, between LEGISWAY ENTERPRISE and other systems managed by Customer

D. Retention period

As Data Controller, Customer shall determine the retention period for Personal Data managed by/in LEGISWAY ENTERPRISE (contract files, disputes, contact identification information, related documents...).

In Cloud mode, the Provider shall make backups and keep them in accordance with the provision of the Agreement, including those of this Schedule. In On-premise mode, Customer is responsible for safeguarding and back upping Customer Data.

Provider as Processor also keeps Customer Data, including, if applicable, Personal Data in the following cases and for the following retention period:

- Personal Data via the support/helpdesk (information that Customer provides for Maintenance tickets): Customer Data including, if applicable, Personal Data shall be deleted from Provider's support databases six (6) months after the expiration of the Agreement; as Data Controller, Customer shall always ensure that no particular Categories of Data are transmitted to Processor when reporting and processing an Anomaly or any incident to Provider's support services (in the form of screenshots, etc.);

- Copy of Customer Data (DUMP) to support/helpdesk : 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 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, Customer Data shall be transmitted to Customer in the agreed format. Provider shall then retain the corresponding databases for two (2) months (or such other period as specified in the Agreement) on its servers before complete destruction.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

In accordance with the Applicable Data Protection Law, Provider shall take the appropriate Technical and Organizational Security Measures ("TOMs"), which shall be assessed on the basis of the state of the art at the time of the conclusion of the Agreement, and shall evaluate such TOMs over time, taking into account the costs of implementation, the nature, scope, context and purposes of the Processing, as well as its likelihood to result in a high risk to the rights and freedoms of Data Subjects.

A. Access control : Buildings

Provider/Processor sites : 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. Customer, as Data Controller, must also ensure that adequate security measures to prevent access to its buildings are implemented.

Provider subcontractor/Sub-processors Sites (CLOUD mode only): On execution of the Agreement, the hosting Sub-processor is CLARANET : its servers and platform are located in France in Equinix Data Center, within a private area for CLARANET. The replicated database server is also located in France, within a private area for CLARANET.

B. Access control : systems

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

Customer, as Data Controller, must also ensure that adequate measures are implemented to secure its passwords and other electronic access information.

C. Access control : Data

Provider, acting as data Processor, 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

Applicative data flows between Customer and Provider are encrypted via the HTTPS protocol.

For exchanges associated with the implementation of LDAP or SSO authentication in the context of Cloud deployments, Provider recommends the use of an IPSEC encrypted tunnel.

When Customer wishes to set up interfaces between the Software and a system of its own in the context of Cloud deployments, Provider also recommends the implementation of an IPSEC encrypted tunnel.

Messages (e-mails) are sent by the platform to inform Users of certain events (due dates, tasks to be performed, etc.). These e-mails are not encrypted, but they do not contain any critical business information and in particular no content (contract, related document, etc.).

As an option, Providers may encrypt certain sensitive data fields (corresponding to sensitive data) in the database. If Customer has paid for this option, Customer and Provider define which fields are encrypted. Those fields are encrypted and decrypted by the application server when they are accessed for reading and writing.

E. Software development

In the development of the Software, Provider implements the good practices recommended by OWASP (www.owasp.org) and more specifically on the recommendations of the "Top 10" project:
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Security tests are performed at regular intervals. The results of these tests are used to continue to limit the remaining risks.

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

F.1 At Provider

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

Personal Data is partitioned. Measures include:

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

« On premise » deployment specific measures

For On premises deployments, the essential processes related to usage and security are Customer's responsibility.

Subprocessing : none in running phase

Backups and restores : Provider recommends the implementation of daily backups. Implementation and verification of those backups are Customer's exclusive liability.

Test/acceptance environment : Provider recommends that Customer have at least two environments on their platform : a production environment, and a test/acceptance environment.

« Cloud » deployment specific measures

Subprocessing *:* On Agreement Effective Date, hosting and outsourcing of Provider servers are sub contracted to CLARANET
CLARANET is ISO-27001certified for the hosting activities provided to Provider.

Backups and restores : Configurations of the application servers are saved daily on the backup infrastructure of CLARANET on a remote site.
The entire Customer database is backed up daily on CLARANET's backup infrastructure at a remote site.
Backups are kept for a duration of four weeks. Backups are not encrypted.

Test/acceptance environment : Provider recommends that Customer have at least two environments on the platform : a production environment, and a test/acceptance environment.

Access filtering by IP address : Independently of the security provided by the identity management solution, the Provider implements for the Customer an access filtering by a list of IP addresses (white list) corresponding to the public IP addresses of the Customer's Internet gateways.

Isolation The physical and logical architecture ensures that Customer works in environment that is isolated and separate from other customers. Each customer has a dedicated database and a dedicated instance of the Tomcat application server.

Security updates : CLARANET monitors security flaws and associated updates and makes regular recommendations to Provider on security updates. These security updates are applied regularly on the basis of the recommendations.

Antivirus protection : an anti-virus solution is deployed and maintained on Provider' Software.

Business continuity plan (BC) *:* A BCR is in place providing for service failover to a secondary datacenter in the evet of a service interruption on the primary server.

Procedure to manage security incident: Provider implements security incident management process with notification of Data breach in accordance to the Data Processing Agreement.

Data erasure *:* In accordance with the provisions of the Agreement.

F.2 At Customer

Managing permissions : LEGISWAY ENTERPRISE integrates by design and by default customizable functions for the protection of Customer Data, enabling Customer to manage the levels of rights to segment the information accessible to Users and to define the appropriate level of protection according to the Personal Data that it will be processing.

User profiles are assigned to Users by Customer administrators when they are declared/registered in the Software.

Directory Data of natural persons are protected within the Software's database in the same way as all Data manipulated in the Software. They are only accessible through the Software by Users who have obtained the corresponding authorizations from the Customer. Customer, as Data Controller, is therefore required to establish confidentiality rules at its own convenience and it is up to Customer to define the levels of User authorisation according to the User profiles.

Tracking : LEGISWAY ENTERPRISE offers an audit trail function that stores in the database of the Customer a set of information about the access and use of each user of the Software. This information includes in particular a log of connections (successful and failed) as well as accessed and/or modified content. This information is accessible to an authorized administrator of the Customer.

Authentication : . Several authentication management modes are available depending on the options to which the Controller has 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).

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

Data encryption : Provider proposes a chargeable option to encrypt certain Data fields (within the database). The objective is that even in the event of unauthorized distribution of the Customer's database, this information will remain inaccessible. When this option is acquired by Customer, the fields in question are encrypted and decrypted by the application server when they are accessed to be read or modified. The encryption keys are managed at the application server level.

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

The Legisway Enterprise system is monitored continuously:

- 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.
- An intrusion detection system is always active and gives real-time warnings.
- A vulnerability scan is performed regularly.

SUB PROCESSORS

On the effective date of the Agreement the following Sub-processors 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	configuration	France	--
S. Blavet	configuration	France	--
Pharmadvize SARL 37 rue d'Amsterdam 75008 Paris	training	France	--
Formateurs, personnes physiques	training	France	--
Claranet SAS* 2 Rue Breguet, 75011 Paris	Hosting and datacenter for Cloud ENTERPRISE	France	Equinix/hosting/France Telecity/hosting /France Telehouse/hosting/France
DELLA AI UK Ltd. at 5 Countess Road, NW5 2NS, London	Provider of Indexing Service And support level 2	France	Orange Business service/ hosting/France
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth	Provider of the service (option) Teamdocs	Germany	Telekom Deutschland GmbH (Scanplus GmbH)/hosting/Germany
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth	Support level 2 Teamdocs (option)	Germany	Toppann Merrill GmbH/software editor and support level 3/Allemagne
Claranet SAS 2 Rue Breguet, 75011 Paris	Hosting and datacenter Mail to Legisway (option)	France	Equinix/hosting/France Telecity/hosting /France
Wolters Kluwer Global business services B.V. Zuidpoolsingel 2, 2408 ZE Alphen aan den Rijn, Pays-Bas	Hosting and datacenter Word2PDF (option)	The Netherlands	Azure, Europe/Hosting

* CLARANET is ISO-27001 certified for its hosting and outsourcing activities