GDPR PRODUCT SHEET (PRODUCTFICHE)
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	Training	France	--

Paris, 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. at 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
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	--