Wolters Kluwer

GDPR PRODUCT INFO 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 Legisway Essentials can be used 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	Address	Purpose of use
Wolters Kluwer Global Business Services	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, The Netherlands	2nd level support and software development
Teleperformance Portugal	Cais dos Argonautas Lote 2.34.01 Lisbon – Portugal	1st level support
Wolters Kluwer Italia	Centro Direzoniale Milanoflori Strada 1, Palazzo 6, 20090 Assago - Italy	2nd & 3rd level support and software development
Salesforce.com EMEA	Floor 26 Salesforce Tower	Tool for follow-up of support tickets

	110 Bishopsgate, London EC2NB 4AY, UK	
Capgemini Nederland	Reykjavikplein 1 3543 KA Utrecht, The Netherlands	Consultancy services for the implementation and development of Salesforce
NTT Europe	Frankfurt Data Center, Russelsheim, Frankfurt, Germany	Data center

9. Transmission of personal data

All Personal Data as included in this Product Sheet will not be passed on except to the above-mentioned Sub-processors and only in the context of the execution of this agreement.