# Productsheet

# Kleos

## 1 Nature of the Processing

Online management software for lawyers.

## 2 Categories of Personal Data that are processed

Wolters Kluwer will process the following categories of Personal Data exclusively in the context of this Addendum:

- Identity data (last name, first name, login name)
- Contact information (address, e-mail, IP address, telephone, fax)
- Behavioural data (user history)

As Controller you have the opportunity to enter additional personal information from your customers in Kleos. Basic fields which are provided in Kleos and may be filled in by you are:

- Identity data (name, address, mobile phone, e-mail, date of birth, etc.)
- Identity data issued by the government (national registration number, etc.)
- Social status (family situation, etc.)
- Financial information (bank account number, etc.)
- You can always add other additional personal data via the "additional fields" function.

## 3 Categories of data subjects involved in the Processing of personal data in Kleos

- clients and partners of the Controller
- shareholders, partners, employees and other staff members of the Controller, including trainees, research assistants, etc;
- other persons whose data are processed by the Controller, such as counterparties.

## 4 Purposes of the processing

Wolters Kluwer stipulates that you can use Kleos for the purposes below:

- Central management of cases, contact data and documents
- Certified connection with the DPA, Digital Platform for Attorneys
- Kleos Connect: secure exchange of your files with your customers and other parties
- Accounting and invoicing: On the basis of the recorded services and costs you automatically draw up your statements of fees and invoices with Kleos, send reminders, make the VAT declaration and create client listings.
- Linking to your internal and external sources
- Extensive search and reporting possibilities
- Exporting information for reports.

## 5 Retention period

As Controller, you yourself determine the retention period of your client information (dossiers, identity data, documents, etc.)

Wolters Kluwer makes a backup of all client 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 make it available to Wolters Kluwer if necessary
- Personal data via support/helpdesk: contacts are anonymised six months after the termination of the contract. As Controller you make sure not to transmit sensible 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 also test environment have both transport and file encryption in place.
  Your permission is requested in advance for this. These data are 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 Agreement: we provide the data in a general and accessible file format. Subsequently we keep the data on our servers for three months.

## 6 Support/helpdesk

To resolve an issue or carry out additional configuration, Wolters Kluwer needs access to the database of the Controller.

- The Controller can give the Wolters Kluwer employee access to Kleos by activating the Support User in the database. The Controller can switch off this option at all times.
- If access to the technical systems of the Contoller is required, Wolters Kluwer 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 Wolters Kluwer. The Controller is responsible for blocking/protecting all confidential information before granting access.

## 7 Security measures

In accordance with the GDPR regulations, Wolters Kluwer will take appropriate technical and organisational measures, to be assessed on the basis of the state of the art at the time the Service Provision 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 Wolters Kluwer 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 access to networks, operational systems, user administration and applications Wolters Kluwer 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 Wolters Kluwer 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, Kleos requires the user to use a password to enter, which ensures the confidentiality of all data entered in the management system. Kleos also offers the possibility of managing the user rights to segment the information accessible within the data controller's office, if the Controller so wishes. The controller is therefore required to establish confidentiality rules within the firm.

## 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:

The Kleos 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 Kleos website is also certified.
- McAfee Security carefully monitors Kleos 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.

## 7.8 Available certification

ISO/IEC 27001 certification

## 8 Sub-processors

The following Sub-processor(s) perform services on behalf of Wolters Kluwer with regard to personal data:

| Name | Address | Purpose of use |
|---|---|---|
| Wolters Kluwer Global Business Services | Zuidpoolsingel 2<br>2408 ZE Alphen aan den Rijn<br>The Netherlands | 2nd level support and software development |
| Teleperformance Portugal | Cais dos Argonautas<br>Lote 2.34.01<br>Lisbon – Portugal | 1st level support |
| Wolters Kluwer Italia | Centro Direzoniale Milanoflori<br>Strada 1, Palazzo 6<br>20090 Assago - Italy | 2nd & 3rd level support and software development |
| Capgemini Nederland B.V. | Reykjavikplein 1<br>3543 KA Utrecht - Nederland | Development support tool |
| Salesforce EMEA Limited | Floor 26 Salesforce Tover<br>110 Bishophsgate<br>London EC2N 4AY - United Kingdom | Tool for follow-up of support tickets |
| T-Systems International GmbH | Data centre Munich/Allach<br>Dauchauer Strasse 665<br>80995 München, Germany<br><br>Data Centre Munich/Eip<br>Elisabeth Selbert Strasse 1<br>80939 München, Germany | Datacenter |

### 1. Transmission of personal data

All Personal Data as included in this product sheet will not be passed on unless to the above-mentioned sub-processors and only in the context of the execution of this agreement.