Wolters Kluwer

GDPR PRODUCT FILE

DLEX

1 Type of processing

Management software for lawyers

2 Categories of Personal Data processed

Wolters Kluwer as Processor will only process the following categories of users' Personal Data in the context of this Addendum:

- Identity data (surname, first name, user name)
- Contact details (address, email address, telephone number, fax number)
- Behavioural data (user history)

As Data Controller you have the option of entering additional personal information about your customers in DLex. Basic fields that are provided in DLex and can be completed by if you wish are:

- Identity data (name, address, mobile phone number, email address, date of birth, etc.)
- Identity data issued by the government (national registration number, passport number, etc.)
- Social status (family situation, etc.)
- Financial data (bank account number, etc.)
- Further personal data can be added using the 'extra fields' function. The title, layout and content of these fields are the responsibility of the Data Controller.

3 Categories of Data Subjects for the processing of personal data in DLex

- Customers and partners of the Data Controller
- Shareholders, employees and other personnel members of the Data Controller, including interns, assistants, etc.;
- Other persons whose data are processed by the Data Controller, such as counterparties.

4 Purposes of processing

Wolters Kluwer intends you to use DLex for the following purposes:

- Central management of files, contact details and documents
- Certified connection with the DPA, Digital Platform for Lawyers
- Extranet/CWA: secure exchange of your files with your customers and other parties
- Accounting and invoicing: on the basis of the recorded services and costs, you can automatically prepare your fee notes and bills with DLex, send out reminders, submit VAT returns and create customer listings.
- Establishing links to your internal and external sources
- Extensive search and reporting options
- Exporting information based on reports etc.

5 Retention period

As Data Controller you yourself determine the retention period of your customers' information (files, identity data, documents, etc.). You are also responsible for protecting and backing up the information on your server.

Personal Data will be processed and retained by Wolters Kluwer for the following periods:

- After the migration of your data from another software package: we do not store any information after migration from the previous software package. The Data Controller is responsible for copying/backing up this information and will make it available to Wolters Kluwer if necessary.
- Personal data via support/help desk: contact information is anonymised six months after the termination of the contract. You are responsible for ensuring that you do not send any sensitive information with a view to resolving your question (screenshot etc.).
- A copy of your data for support/helpdesk: in order to resolve a technical problem we may transfer a copy of part of your data to a test environment. Your consent will be requested for this beforehand. These data will only be used to resolve the problem that has occurred and will be removed from the test environment after the intervention has been carried out.

6 Support/helpdesk

In order to resolve a problem or perform an additional configuration, Wolters Kluwer must have access to the DLex interface and/or the Data Controller's PC, and sometimes needs direct access to the database and DLex server in more complex cases.

- If access to the Data Controller's technical systems is required, Wolters Kluwer will be given remote access to the Data Controller's computer. Remote access requires activation by the customer by entering a code provided by Wolters Kluwer. The Data Controller is responsible for closing/restricting all confidential information before granting access.
- If access to the server or database is necessary, the Data Controller can grant access to the Wolters Kluwer employee under certain conditions:
    - Such access must not be permanent, but must be capable of being activated on request.
    - For a faster solution it is preferable for the connection information to be static, known to the IT manager and DLex and capable of being activated if necessary. This connection information must be stored in secure environments by IT subcontractors and DLex and must only be accessible to those who need the information.
    - In order not to delay the handling process, all requesters of support must be aware of the activation/deactivation procedure.
- Wolters Kluwer will not make any changes to the database without the supervision of the Data Controller or the Data Controller's IT service provider (if the Data Controller grants this right in writing).
- Wolters Kluwer will not make any changes to the Data Controller's server: the right to do so is reserved for the Data Controller or its IT service provider.

! **Important!** The DLex support team may not under any circumstances install a Microsoft patch or manually download and install a new DLex version instead of having the Data Controller or its IT partner do so. The only two methods allowed for a DLex update are as follows:

- activation directly by the Data Controller or its IT provider via the DLex upgrader function (verification by IT recommended)
- activation via an automatic batch function on predetermined data and only if experience has shown this method to be reliable for the Data Controller's IT environment. In the event of problems, DLex support may assist the Data Controller's IT partner, in its presence, with this type of operation if the methods mentioned above are not effective.

7 Security measures

Wolters Kluwer will, in accordance with the provisions of GDPR, take appropriate technical and organisational measures, to be assessed in light of the state of technology at the time of conclusion of the Service Provision Agreement, and will evaluate these measures after a period of time, taking account of

costs of implementation, type, scope, context and objectives of the processing and the risk of differences in the degree of probability and gravity 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 as Processor is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.

As Data Controller you must ensure that adequate security and access measures are in place for your buildings.

7.2 Access control: systems

For access to networks, operational systems, user administration and applications, the Processor requires the necessary authorisations: advanced password procedures, automatic time-out and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.

As Data Controller you must ensure that adequate security and access measures are in place for your buildings.

7.3 Access control: data

Access to the data is controlled by Wolters Kluwer itself by organisational measures: user administration and user accounts with specific access, personnel trained in data processing and security, separation of operational systems and test environments, allocation of specific rights and recording of history of use, access and deletion.

As Data Controller you must ensure that adequate measures are taken to protect data and documents.

7.4 Ability to ensure continued confidentiality, integrity, availability and resilience of processing systems and services:

Access control for personal data must adhere to the guidelines for internal controls, including the organisation's policy on access to information, implementation of a user administration system and access rights, the creation of awareness among employees about handling information and their passwords, network access controls, including separation of sensitive networks, and access controls to the operating system and underlying applications. Specifically, the measures include:

- Written/programmed authorisation structure;
- Differentiated access rights (including for reading, editing, deleting);
- Definition of roles;
- Logging/auditing;
- Separation of personal data. The measures include:
    - Separation of functions (production/test data);
    - Separation of particularly sensitive data.
- Purpose limitation/compartmentalisation;
- A policy/measures to guarantee separate storage, modification, deletion and transfer of data.

As Data Controller, the DLex user must enter a password, which guarantees the confidentiality of all data entered in the management system. DLex also offers the option of managing user rights in order to segment the information that is accessible within your office if you wish. It is then the Data Controller's responsibility to secure access to the data on the server and databases, since DLex is hosted on the Data Controller's Network.

The Data Controller must therefore establish confidentiality rules within the office on its own initiative.

7.5 Ability to restore the availability of and access to the Personal Data on a timely basis in the event of a physical or technical incident:

Data are stored on the Data Controller's server and fall under its responsibility.

7.6 Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure processing security:

The Processor ensures that regression tests are performed to maintain compatibility with the GDPR rules prior to the delivery of each new version of DLex.

Due to the technology used for DLex (i.e. client-server), the responsibility for technical and organisational maintenance lies entirely with the Data Controller, who must test and evaluate the technical and organisational measures taken on an ongoing basis.

8 Subprocessors

The following Subprocessor(s) provide(s) services by order of Wolters Kluwer with regard to Personal Data:

Name	Address	Aim of use
CAPTEL	Rue Grétry 50/096 4020 Liège Belgium	'Overflow support' – reception of support and other first-line reports in the event of overflow or unavailability
Capgemini	Capgemini Nederland B.V. Reykjavikplein 1 3543 KA Utrecht - The Netherlands	Consultancy for implementation and development of Salesforce
Salesforce	Salesforce EMEA Limited Floor 26 Salesforce Tower 110 Bishopsgate London EC2N 4AY - United Kingdom	Tool for support tickets
Pluritech	Franklin Rooseveltlaan 26a – 1800 Vilvoorde - Belgium	Test servers delivered for tests in TS client configuration.
Qlik	France Headquarters Office 93 avenue Charles de Gaulle 92200 Neuilly sur Seine - FRANCE	Partner for module reports

1. **Transmission of Personal Data**

   No Personal Data as included in this product file are transmitted other than to the above-mentioned Subprocessors and only in connection with the performance of the agreement.