Wolters Kluwer

GDPR PRODUCT INFO SHEET

Adsolut Windows Application

1. Nature of processing

Comprehensive accounting and ERP software for accountants and SMEs.

2. Categories of Personal Data processed

The Processer will only process the following categories of Personal Data in the context of this Addendum:

☒ 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.)
☒ contact information (address, email address, IP address, IMEI, etc.)
☒ social status (position at work, position within the community, family situation, etc.)
☒ financial information (bank account numbers, loans, mortgages, investments, payment behaviour, ratings, etc.)

3. Categories of Data Subjects

☒ Controller's customers
☒ Controller's own employees

4. Purposes of processing

☒ Accounting and legal obligation
☒ Fiscal obligation
☒ Obligation FPS Economy
☒ finance
☒ purchasing: supplier management
☒ delivery of goods or services
☒ direct marketing
☒ other advertising or marketing purposes
☒ supplier management
☒ business analytics

As part of our ongoing efforts to improve the quality and functionality of our software/product, we collect and analyse data on the use of our products. The data collected is used exclusively for the following purposes:

- Identifying and resolving technical problems and bugs
- Optimising the user experience and interface
- Developing new features and improvements tailored to user needs and preferences
- Perform general product analysis to improve the efficiency and effectiveness of the software

5. Retention period

Personal Data are currently processed and retained for the following periods:

Entered Personal Data: If Adsolut is hosted by the Processor, entered Personal Data will be kept for an unlimited period. If Adsolut is hosted by the Controller, the retention period is determined by the Controller.

Personal Data via helpdesk support: These are kept for an unlimited period.

Wolters Kluwer strives for the continuous improvement of its services and will therefore bring these retention periods in line with the applicable legislation.

If Adsolut is in a location hosted by the Processor, the data will be deleted after the termination of the contract.

6. Security measures

Technical and organisational measures can be regarded as state-of-the-art at the time of conclusion of the Service Provision Agreement. The Processor will evaluate technical and organisational measures over time, taking account of implementation costs, nature, scope, context and objectives of processing, and differences in the likelihood and the severity of risks for the rights and freedoms of natural persons.

If the product is not in a location hosted by the Processor, responsibility for technical and organisational measures lies with the Controller.

Detailed technical and organisational measures:	
Access control: buildings	Access to Wolters Kluwer buildings is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.
Access control: systems	Access to networks, operational systems, user administration and applications require the necessary authorisations: advanced password procedures, automatic time-out and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.
Access control: data	Access to the data themselves on the part of Wolters Kluwer is controlled by organisational measures: user administration and user accounts with specific access, personnel trained in data processing and security.
Available certification	ISO/IEC 27001 certification

If Adsolut is in a hosted location, these measures are applied by the Processor's Sub-processor. The following measures apply:

Detailed technical and organisational measures:	
Access control: buildings	Access to the Sub-processor's buildings is controlled by both technical and organisational measures: access control with personalised badges, electronic locking of doors, reception procedures for visitors.
Access control: systems	Access to networks, operational systems, user administration and applications require the necessary authorisations: advanced password procedures, automatic time-out and blocking for incorrect passwords, individual accounts with histories, encryption, hardware and software firewalls.
Access control: data	Access to the data themselves is controlled 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.

Pseudonymisation of data:	There is no pseudonymisation of data.
Encryption of data:	Access to the data is gained exclusively via secure protocols. Passwords are stored hashed.
Ability to ensure continued confidentiality, integrity, availability and resilience of processing systems and services:	Separation of production and test environment, separation of specific sensitive data, automatic back-up, advanced password procedures, specific usage rights, recording of history.
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:	Uninterrupted power supply, backup data centres at different locations, security systems in the event of fire or water damage, extinguishing systems, fire-resistant doors, fire detectors.
Process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures to ensure processing security:	24/7 monitoring, dual power supply, emergency generators, fire detection and extinguishing systems, automatic backup systems, periodically scheduled systems maintenance.
Available certification:	ISO-27001

7. Sub-processors

The following Sub-processors carry out services relating to Personal Data on behalf of Wolters Kluwer:

Name	Address	Purpose of use
ConXion BV	Hoogstraat 134 8540 Deerlijk BE0458.974.603	Implementation of the user agreement, maintenance and development of the cloud platform.
Penneo A/S	Enghavevej 40, 4th floor 1674 Copenhagen V Denmark Central Business Register (CVR) no.: 35633766	Processing of documents presented to the customer's customer for signature.

8. Transfer of personal data

No transfer of personal data takes place.