Kleos

is the safest and securest environment for your data.

To us, Security is a priority. We stay up-to-date with leading industry standards and we and our partners are certified for that.

Kleos is the safest and securest environment for your data.
The data of your firm and your clients are protected and isolated so to be accessed only by you. That way you can ensure the highest privacy and confidentiality standards to your own clients.

The data are held by a certified company of Deutsche Telekom, with servers located in Germany and compliant with EU data privacy rules and highest security market standards. The farm is continuously monitored 24/7, **with restricted and controlled access to buildings, systems and servers that are protected from intrusions and accidents. We ensure High Availability, Business Continuity and Disaster Recovery, and nightly backup for your data resilience to incidents.** Kleos is also certified with daily security audits of website and of HTTPS encrypted data transmission:

McAfee SECURE

Norton SECURED powered by Symantec

Beside hackers, the majority of security issues are due to human error or infidelities. We place as much emphasis on "procedures and people" security management as on the technical side: this is why we are certified ISO 27001.

ISO 27001

We place as much emphasis on "procedures and people" security management as on the technical side: this is why we are also certified ISO 27001. All services around Kleos - support, quality analysis and infrastructure management – are governed by an information security management system certified from BSI authority that prevent unauthorized data access.

The safest and securest environment for your data.

SECURE AND CERTIFIED WEBSITE

Web site is protected against virus, malware, and fishing by professional tools from McAfee and Norton, examining also other kinds of vulnerability.

SECURE AND CERTIFIED HTTPS CONNECTION DURING DATA TRANSFER

HTTPS Data transmission is encrypted with a 2048-bit PKI Certificate **and certified by Norton.**

Authentication

SECURE WK DATA CENTER IN TOP-RANKED, CERTIFIED FARM IN EU

- **Data center located in Germany**, with dedicated hosting for Wolters Kluwer by T-Systems (Deutsche Telekom)
- Compliant with **EU data privacy rules**
- Certified at highest security market standards and reports (**ISO 27011, SAS-70 Type II**)
- High Availability, Business Continuity and 24/7 system monitoring
- **Encrypted Backup and Disaster Recovery** replicas on a remote site
- **No data access for unauthorized people**
- Each customer's data are isolated with a private instance
- **Buildings and servers protected from intrusion and attacks**

Wolters Kluwer

FAQ

Is the cloud secure enough?

Security is actually increased when using cloud solutions due to strict security standards that cloud providers must adhere to, in addition to the regular security audits and reporting. This means no more worrying about lost laptops with confidential data and treacherous hacking threats, or lost backup. And Kleos ensures top-ranked and certified security with data hosting, transmission and access.

Do you perform controls on Kleos security?

Kleos system is Continuously monitored

- 24/7 accurate Monitoring checks both Health of the System and Performances of the Application customer by customer.
- Intrusion tests are performed every year by an external independent company
- Moreover, intrusion detecting system is always on and gives real time alarms
- Kleos website is also certified:
- McAfee security rigorously audits Kleos every day
    - *Certifies that the web site is secure and resistant to virus and intrusions, protected by hacker attacks on servers and transmissions.*
    - *We are notified in real time about any undergoing risk so that we can immediately block any attack.*
    - *See certificate at https://www.mcafeesecure.com/verify?host=kleos.wolterskluwer.com*
- Norton Symantec continuously monitor our encrypted data transmission via SSL certificate
    - *A monthly 'vulnerability scan' is performed and reported to us.*
    - *See certificate at https://trustsealinfo.verisign.com/splash?form_file=fdf/splash.fdf&dn=kleos.wolterskluwer.com&lang=en*
- Kleos data access is limited, with control of people and processes in the farm and in our offices
    - *Both T-system farm and Wolters Kluwer are certified ISO 27001*
    - *We have implemented more than one hundred controls on Kleos services based on ISO 27001 – Annex A*
    - *We have specific ISO 27001 procedures to manage security in Kleos services like third level support, infrastructure, quality assurance*

Is the value of certifications expiring at some moments?

- No.
- McAfee and Norton Symantec ensure continuous daily/monthly checks of Kleos website and data transmission.
- As long as we keep our level of security, Kleos will be certified.
- If some attack should be done, McAfee and Norton immediately alert us so that we can act and block it, to keep your data secure.
- Data center certifications are renewed and verified every year Our ISO 27001 certification on Kleos service is verified, renewed and extended every year

Where are my data hosted, and how are they protected?

Kleos uses the highest security data hosting services of Deutsche Telekom/T-Systems farm:

- T-Systems is a certified company of Deutsche Telekom, with servers located in EU (in Germany) and compliant with EU data privacy rules and highest security market standards
- Grants certified international security, aligned with highest market standards (ISAE 3470, ISO/IEC 27001, SAS-70 Type II)
- Continuously monitored 24/7
- High Availability, Business Continuity and Disaster Recovery
    - *Customers' Data are always accessible: every Kleos technology component is, at any layer, fully redundant.*
    - *Customer's Documents can be accessed also in the remote case of service unavailability, thanks to a 'safe mode' service.*
    - *Customer's data are replicated to another T-System "mirrored" datacenter (geographically separated, in Germany as well), to be recovered in case of disaster in the main datacenter.*
- Incident, problem and change management regarding Kleos infrastructure is managed through specific processes inspired to ITIL v3 to protect data.
- Customer's data are always backed up to be protected by any type of accidents.
- Restricted and controlled access to all buildings in datacenters protect from intrusions and accidents
    - *Access to the buildings are under the most strict rules and allowed only to authorized people owning a personalized smartcard.*
    - *Buildings are designed to withstand to C4 bombardment, high raid security.*
- Restricted and controlled access to systems and servers:
    - *Access to systems and servers is under the most strict rules and allowed only to authorized administrators.*
    - *Administrators, in order to access the systems, need to possess a specific account.*
    - *They can access system only for maintenance reasons and data only under explicit authorization by the customer.*
    - *Any access is logged and permanently saved through an external certified service compliant with the Privacy Law.*

What happens to my data during the transfer to the farm?

Kleos grants clients' data access and communications (upload / download) encryption and isolation

- Data from the client to the server are encrypted with a 2048-bit PKI Certificate.
- Traffic's hijack techniques are prevented.
- Data are isolated, each customer has a physical private instance. Nothing is shared with other customers.
- Access to proper Customer's data from public Internet is ultimately controlled by the application itself with a set of credential
- Firewall, virus and data corruption protection keep from intrusions data coming inward the Datacentre is filtered by specialized hardware devices performing as Stateful Packet Inspection (SPI) as Intrusion Detection (ID).