

Kleos

is de best beveiligde omgeving voor uw gegevens.

Voor ons is beveiliging een prioriteit. Wij volgen de hoogste standaarden op de markt, en zowel wijzelf als onze partners zijn hiervoor gecertificeerd.

Kleos is de best beveiligde omgeving voor uw gegevens.

De gegevens van uw kantoor en van uw cliënten worden zodanig beschermd en geïsoleerd dat alleen u ze kunt opvragen. Zo kunt u uw cliënten de hoogste normen op het vlak van privacy en vertrouwelijkheid waarborgen.

De gegevens worden bewaard door een gecertificeerde onderneming van Deutsche Telekom, met servers in Duitsland. Deze firma leeft de EU-regels inzake gegevensbescherming na en voldoet aan de hoogste beveiligingsnormen op de markt. De farm wordt 24/7 continu bewaakt, met toegangsbeperking en -controle voor de gebouwen, systemen en servers, die beschermd zijn tegen inbraak en ongevallen. Wij waarborgen een hoge beschikbaarheid, bedrijfscontinuïteit, disaster recovery en nachtelijke back-ups om sneller te kunnen reageren op incidenten. Kleos is ook gecertificeerd met dagelijkse beveiligingsaudits van de website en https-versleutelde datatransmissie.



ISO 27001

Afgezien van hackers zijn menselijke fouten of onnauwkeurigheden de meest voorkomende oorzaken van beveiligingsproblemen. Wij hechten evenveel belang aan het beveiligingsmanagement van "procedures en mensen" als aan het technische aspect: daarom behaalden wij ook het ISO 27001-label. Om onbevoegde gegevenstoegang te voorkomen, worden alle diensten rond Kleos - ondersteuning, kwaliteitsanalyse en infrastructuurbeheer - geregeld door een systeem voor informatiebeveiligingsmanagement met BSI-certificatie.



De best beveiligde omgeving voor uw gegevens



BEVEILIGDE EN GECERTIFICEERDE WEBSITE

De website is tegen virussen, malware en phishing beveiligd met professionele tools van McAfee en Norton, die ook andere vormen van kwetsbaarheid onderzoeken.



BEVEILIGDE EN GECERTIFICEERDE HTTPS-VERBINDING TIJDENS GEGEVENSVERZENDING

De HTTPS-datatransmissie is versleuteld met een 2048-bit PKI-certificaat en is gecertificeerd door Norton.



Authenticatie



Firewall

BEVEILIGD WK-DATACENTER IN EEN VAN DE BESTE GECERTIFICEERDE FARMS IN DE EU

- **Datcenter in Duitsland**, met specifieke hosting voor Wolters Kluwer door T-Systems (Deutsche Telekom)
- In overeenstemming met **EU-regels voor gegevensbescherming**
- Gecertificeerd volgens de hoogste standaarden op de beveiligingsmarkt (**ISO 27011, SAS-70 Type II**)
- Hoge beschikbaarheid, bedrijfscontinuïteit en 24/7 systeembewaking
- **Versleutelde back-up en disaster recovery** replica's op een externe site
- **Geen gegevenstoegang voor onbevoegden**
- De gegevens van elke cliënt zijn geïsoleerd met een private instance
- **Gebouwen en servers beveiligd tegen inbraak en aanvallen**



FAQ

Is de cloud veilig genoeg?

De veiligheid is vele malen hoger bij het gebruik van Cloud-oplossingen, omdat cloud providers naast de gewone beveiligingsaudits en -rapportages strengere beveiligingsnormen moeten naleven. U hoeft zich dus geen zorgen te maken over verloren laptops met vertrouwelijke gegevens, verraderlijke hackingpraktijken of verloren back-ups. Kleos staat bovendien voor hoogwaardige en gecertificeerde beveiliging met datahosting, -transmissie en -toegang.

Controleert u de beveiliging van Kleos?

Het Kleos systeem wordt ononderbroken bewaakt

- In het kader van de 24/7-monitoring worden zowel het systeem als de prestaties van de toepassing voor elke cliënt afzonderlijk nauwkeurig gecontroleerd.
- Ieder jaar voert een onafhankelijke externe onderneming beveiligingstests uit.
- Bovendien is het inbraakdetectiesysteem altijd actief en geeft het realtime-waarschuwingen.
- De Kleos-website is ook gecertificeerd.
- McAfee security controleert Kleos elke dag nauwkeurig:
 - *Certificeert dat de website beveiligd is, bestand is tegen virussen en inbraakpogingen, en beschermd is tegen aanvallen van hackers op servers en datatransmissie.*
 - *Wij worden in real time ingelicht over eventuele risico's, zodat wij aanvallen onmiddellijk kunnen blokkeren.*
 - *Zie certificaat op <https://www.mcafeesecure.com/verify?host=kleos.wolterskluyer.com>*
- Norton Symantec controleert ononderbroken onze versleutelde datatransmissie via het SSL-certificaat
 - *Maandelijks vindt een kwetsbaarheidsscan plaats en ontvangen wij het bijbehorende rapport.*
 - *Zie certificaat op https://trustsealinfo.verisign.com/splash?form_file=fd/splash.fdf&dn=kleos.wolterskluyer.com&lang=en*
- De toegang tot de gegevens in Kleos is beperkt. Wij controleren mensen en processen bij onze provider en in onze kantoren.
 - *Zowel T-systems als Wolters Kluwer zijn ISO 27001 gecertificeerd*
 - *Wij voerden meer dan honderd controles uit op Kleos-diensten op basis van ISO 27001 – Bijlage A*
 - *Wij beschikken over specifieke ISO 27001 procedures om de beveiliging te beheren in Kleos diensten zoals derdelijns ondersteuning, infrastructuur- en kwaliteitsborging*

Zullen de certificaten vervallen?

- Nee.
- McAfee en Norton Symantec voeren onderbroken dagelijkse/maandelijkse controles van de Kleos-website en datatransmissie uit.
- Zolang wij ons beveiligingsniveau behouden, zal Kleos gecertificeerd zijn.
- Bij een aanval brengen McAfee en Norton ons onmiddellijk op de hoogte zodat wij de aanval kunnen blokkeren om uw gegevens veilig te houden.
- De certificaten van het datacenter worden jaarlijks hernieuwd en gecontroleerd. Onze ISO 27001-certificatie voor de Kleos diensten wordt jaarlijks gecontroleerd, hernieuwd en uitgebreid.



Waar worden mijn gegevens gehost en hoe worden ze beschermd?

Kleos gebruikt de best beveiligde datahosting-diensten van de Deutsche Telekom/T-Systems

- T-Systems is een gecertificeerde onderneming van Deutsche Telekom, met servers in Duitsland. Deze firma leeft de EU-regels inzake gegevensbescherming na en voldoet aan de hoogste beveiligingsnormen op de markt.
- Biedt gecertificeerde internationale beveiliging, afgestemd op de hoogste standaarden op de markt (ISAE 3470, ISO/IEC 27001, SAS-70 Type II)
- Continue monitoring 24/7
- Hoge beschikbaarheid, bedrijfscontinuïteit en disaster recovery
 - *Uw data zijn altijd toegankelijk: elke technologische component van Kleos, op welke laag ook, is volledig overbodig.*
 - *Dankzij een veilige modus zijn uw documenten ook toegankelijk als de dienst onbeschikbaar zou zijn, wat hoogst onwaarschijnlijk is.*
 - *Uw gegevens worden continu gekopieerd naar een ander T-System datacenter (geografisch gescheiden, ook in Duitsland) en kunnen in een noodsituatie van daaruit worden hersteld.*
- Om de gegevens te beschermen, worden Incidenten, problemen en verandering met betrekking tot Kleos infrastructuur beheerd via specifieke processen, gebaseerd op ITIL v3.
- Voor een betrouwbare bescherming tegen ongevallen van welke aard ook wordt er altijd een back-up gemaakt van uw gegevens.
- Beperkte en gecontroleerde toegang tot alle gebouwen in datacenters beschermen tegen inbraak en ongevallen
 - *Er gelden strenge toegangsregels. De gebouwen zijn alleen toegankelijk voor bevoegde personen met een gepersonaliseerde smartcard.*
 - *De gebouwen zijn bestand tegen bombardementen met C4 en hebben een hoogwaardige RAID-beveiliging.*
- Beperkte en gecontroleerde toegang tot systemen en servers
 - *De toegang tot systemen en servers is aan de strengste regels onderworpen en wordt alleen verleend aan gemachtigde beheerders.*
 - *Om toegang te krijgen tot de systemen, moeten beheerders over een specifiek account beschikken.*
 - *Zij kunnen zich alleen voor onderhoudsredenen toegang verschaffen tot de systemen. Toegang tot gegevens is alleen mogelijk met de uitdrukkelijke toestemming van de cliënt.*
 - *Elke toegang wordt vastgelegd en blijvend opgeslagen via een gecertificeerde externe dienst die de privacywetgeving naleeft.*

Wat gebeurt er met mijn gegevens tijdens de overbrenging naar de farm?

Kleos biedt cliënten gegevenstoegang, versleutelde communicatie (uploaden/ downloaden) en isolatie

- Een PKI-certificaat met 2048 bits-sleutel bewaakt de verzending van de gegevens van de cliënt naar de server.
- Hijack-pogingen worden voorkomen.
- De gegevens worden geïsoleerd, elke cliënt heeft zijn fysieke private instance. Niets wordt gedeeld met andere cliënten.
- De toegang tot de eigen cliëntgegevens vanaf het openbare internet wordt uiteindelijk door de toepassing zelf gecontroleerd aan de hand van een reeks aanmeldingsgegevens.
- Firewall, antivirussysteem en bescherming tegen datacorruptie bieden beveiliging tegen inbraakpogingen. Gegevens die in het datacenter aankomen, worden gefilterd door gespecialiseerde hardware-apparatuur die procedures zoals Stateful Packet Inspections (SPI) en Intrusion Detection (ID) uitvoert.