Kleos

přináší nejbezpečnější a nejzabezpečenější prostředí pro Vaše data.

Zabezpečení je pro nás prioritou. Držíme krok s nejvyššími standardy v odvětví a stejně jako naši partneři, jsme i my držiteli certifikátů dosvědčujících tuto skutečnost.

Kleos přináší nejbezpečnější a nejzabezpečenější prostředí pro Vaše data.
Data Vaší firmy a Vašich klientů jsou chráněna a izolována tak, abyste k nim měli přístup pouze Vy. Tímto způsobem můžete svým klientům zajistit nejvyšší standard soukromí a důvěrnosti.

Data má v úschově certifikovaná společnost skupiny Deutsche Telekom vlastnící servery v Německu, které splňují předpisy EU o ochraně soukromí dat a nejvyšší standardy v oblasti zabezpečení. Serverová farma je trvale monitorována 24 hodin denně, 7 dnů v týdnu, přičemž **přístup do budov, systémů a serverů chráněných před vniknutíma mimořádnými událostmi je omezen a kontrolován. Zajišťujeme vysokou dostupnost, pracovní kontinuitu a obnovu dat v případě havárie, stejně jako noční zálohování na ochranu Vašich dat pro případ mimořádných událostí.** Kleos je také prověřován každodenními bezpečnostními audity internetových stránek a šifrovaného přenosu dat pomocí protokolu HTTPS:

McAfee SECURE

Norton SECURED powered by Symantec

Vedle hackerů je většina bezpečnostních problémů způsobena lidským selháním nebo porušením pravidel.
Stejný důraz jako na technickou stránku klademe v záležitostech zajištění bezpečnosti na „postupy a lidský aspekt“ - proto jsme také získali certifikát ISO 27001.

ISO 27001

Stejný důraz jako na technickou stránku klademe v záležitostech zajištění bezpečnosti na „postupy a lidský aspekt“ – proto jsme také získali certifikát ISO 27001. Všechny služby související se systémem Kleos – podpora, analýza kvality a správa infrastruktury – podléhají systému řízení informační bezpečnosti, který je certifikován organizací BSI a chrání před neoprávněným přístupem k datům.

Nejbezpečnější a nejzabezpečenější prostředí pro Vaše data.

ZABEZPEČENÉ A CERTIFIKOVANÉ INTERNETOVÉ STRÁNKY

Internetové stránky jsou chráněny před viry, malwarem a phishingem pomocí profesionálních nástrojů vyvinutých společnostmi McAfee a Norton, které věnují pozornost nejrůznějším druhům zranitelných míst.

ZABEZPEČENÉ A CERTIFIKOVANÉ SPOJENÍ POMOCÍ PROTOKOLU HTTPS BĚHEM DATOVÉHO PŘENOSU

Přenos dat pomocí protokolu HTTPS je šifrován certifikátem 2048-bit PKI **a ověřen organizací Norton.**

ZABEZPEČENÉ DATOVÉ CENTRUM WOLTERS KLUWER NA ŠPIČKOVÉ CERTIFIKOVANÉ FARMĚ V EU

- **Datové centrum v Německu** s dedikovaným hostingem pro Wolters Kluwer od společnosti T-Systems (Deutsche Telekom)
- Splňuje **pravidla EU o ochraně soukromí dat.**
- Certifikované podle nejvyšších standardů a zpráv v oblasti zabezpečení (**ISO 27011, SAS-70 Typ II**)
- Vysoká dostupnost, pracovní kontinuita a nepřetržité monitorování systému 24 hodin denně, 7 dnů v týdnu
- **Šifrované zálohy a repliky pro obnovu dat v případě havárie** uložené na vzdáleném místě
- **Zákaz přístupu neoprávněných osob k datům**
- Data každého zákazníka jsou izolována v soukromí
- **Budovy a servery chráněné před vniknutím a útoky**

FAQ

Je cloud dostatečně zabezpečený?

Bezpečnost je při používání cloudových řešení ve skutečnosti vyšší z důvodu přísných bezpečnostních standardů, které musí poskytovatelé cloudů vedle podstupování pravidelných bezpečnostních auditů a podávání zpráv splňovat. To znamená, že je zbytečné se stresovat kvůli ztracenému laptopu s důvěrnými daty, kvůli ošidné hrozbě útoku hackerů nebo kvůli ztracené záloze. Kleos zajišťuje špičkové certifikované zabezpečení s datovým hostingem, přenosem a přístupem.

Kontrolujete zabezpečení systému Kleos?

Systém Kleos je trvale monitorován

- 24 hodin denně, 7 dnů v týdnu – provádějí se pečlivé kontroly spolehlivosti systému a výkonu aplikace pro jednotlivé zákazníky.
- Každý rok testuje nezávislá externí společnost možnosti vniknutí.
- K tomu všemu je vždy zapnutý systém detekce vniknutí, který spouští poplašné signály v reálném čase.
- Internetové stránky Kleos jsou také certifikovány:
- McAfee každý den provádí pečlivé kontroly zabezpečení systému Kleos.
    - *Ověřuje, zda jsou internetové stránky zabezpečené a chráněné před viry a vniknutím a zda jsou servery a přenosy chráněné před útoky hackerů.*
    - *Upozornění na rizika dostáváme v reálném čase, abychom mohli okamžitě zabránit případnému útoku.*
    - *Certifikát naleznete zde*
- Norton Symantec nepřetržitě monitoruje naše zašifrované datové přenosy používající certifikát SSL.
    - *Každý měsíc je provedena kontrola zranitelnosti, o které následně dostaneme zprávu.*
    - *Certifikát naleznete zde*
- Přístup k datům v systému Kleos je omezen, týká se osob a procesů na serverové farmě a v našich kancelářích.
    - *Serverová farma společnosti T-system i společnost Wolters Kluwer jsou držiteli certifikátu ISO 27001.*
    - *Bylo provedeno více než sto kontrol služeb systému Kleos podle normy ISO 27001 – příloha A*
    - *Pro zajištění bezpečnosti služeb systému Kleos používáme určité postupy podle normy ISO 27001, jako je podpora třetí úrovně, infrastruktura nebo zabezpečování kvality.*

Může platnost certifikace v některých momentech vypršet?

- Ne.
- McAfee a Norton Symantec zajišťují trvalé denní/měsíční kontroly internetových stránek systému Kleos a přenosu dat.
- Dokud udržíme tuto úroveň zabezpečení, zůstane Kleos certifikován.
- Pokud by se schylovalo k nějakému útoku, McAfee a Norton by nás okamžitě upozornily, abychom mohli útoku zabránit, a tím zajistit, že Vaše data zůstanou v bezpečí.
- Certifikace datového centra se obnovují a ověřují každý rok. Certifikace služeb systému Kleos podle normy ISO 27001 je také každý rok ověřována a prodlužována.

Kde jsou moje data hostována a jak jsou chráněna?

Kleos používá služby datového hostingu serverové farmy Deutsche Telekom/T-Systems s nejvyšším zabezpečením:

- T-Systems je certifikovaná společnost skupiny Deutsche Telekom vlastnící servery v EU (Německu), které splňují předpisy EU o ochraně soukromí dat a nejvyšší standardy v oblasti zabezpečení.
- Certifikované mezinárodní zabezpečení, splňuje nejvyšší standardy v odvětví (ISAE 3470, ISO/IEC 27001, SAS-70 Typ II)
- Trvalé monitorování 24 hodin denně, 7 dnů v týdnu
- Vysoká dostupnost, pracovní kontinuita a obnova dat v případě havárie
    - *Data zákazníků jsou vždy dostupná: všechny komponenty technologie Kleos na všech úrovních jsou zcela redundantní.*
    - *Přístup k dokumentům zákazníka je možný také v případě nedostupnosti služby, a to díky službě „bezpečný režim".*
    - *Data zákazníka jsou replikována do jiného („zrcadlového") datového centra společnosti T-System (geograficky odděleného, nacházejícího se také v Německu) pro účely obnovy v případě havárie v hlavním datovém centru.*
- Řízení v případě mimořádných událostí, problémů a změn týkajících se infrastruktury systému Kleos odpovídá specifickým procesům vycházejícím z ITIL v3 ohledně ochrany dat.
- Data zákazníka jsou vždy zálohována za účelem ochrany při jakýchkoli mimořádných událostech.
- Omezený a kontrolovaný přístup do všech budov v datových centrech zabezpečuje ochranu před vniknutím a mimořádnými událostmi.
    - *Přístup do budov podléhá nejpřísnějším pravidlům a je umožněn pouze oprávněným osobám, které jsou držiteli příslušné osobní čipové karty.*
    - *Budovy jsou vyprojektovány tak, aby odolaly bombardování stupně C4, a jsou vysoce zabezpečeny proti přepadení.*
- Omezený a kontrolovaný přístup k systémům a serverům:
    - *Přístup k systémům a serverům podléhá nejpřísnějším pravidlům a je umožněn pouze oprávněným správcům.*
    - *Správci potřebují mít pro přístup do systémů specifický účet.*
    - *Do systému mohou vstupovat pouze pro účely údržby a přístup k datům je jim umožněn pouze na základě výslovného oprávnění uděleného zákazníkem.*
    - *Každý přístup je evidován a záznam o něm je trvale uložen prostřednictvím externí certifikované služby v souladu se zákonem o ochraně soukromí.*

Co se děje s mými daty během přenosu na serverovou farmu?

Kleos zajišťuje přístup, stejně jako zašifrování a izolaci klientových dat při komunikaci (nahrávání/stažení).

- Data přenášená od klienta na server jsou zašifrována pomocí certifikátu 2048-bit PKI.
- Jsou přijata opatření pro prevenci únosu dat při jejich přenosu.
- Data jsou izolována, každý zákazník má svůj soukromý fyzický prostor. Nic není sdíleno s žádnými jinými zákazníky.
- Přístup k řádným datům zákazníka z veřejné internetové sítě je nakonec kontrolován samotnou aplikací s řadou prvků.
- Firewall, antivirový program a program na ochranu dat před poškozením chrání data přicházející do datového centra před narušením. Data přicházející do datového centra jsou filtrována speciálními hardwarovými zařízeními, která provádějí stavovou firewallovou kontrolu (SPI) a detekci narušení (ID).

Wolters Kluwer ČR, a. s., U Nákladového nádraží 6, 130 00 Praha 3
tel: 246 040 400 / e-mail: kleos@wolterskluwer.cz / www.kleos.cz