# Kleos

# Kleos – software pro komplexní správu advokátních kanceláří V souladu s GDPR

## 1 Povaha zpracování

Online software pro správu agendy advokátů.

## 2 Kategorie zpracovávaných osobních údajů

Wolters Kluwer zpracovává následující typy osobních údajů výhradně v kontextu této přílohy:

- Údaje o osobě (jméno, příjmení, přihlašovací jméno),
- kontaktní informace (adresa, email, IP adresa, telefon, fax),
- data o chování (historie uživatelů).

Jako Správce máte možnost ukládat do Kleosu další osobní údaje o svých zákaznících. Základní pole, která jsou v Kleosu k dispozici a mohou být vámi vyplněna, jsou:

- Osobní údaje (jméno, adresa, mobilní číslo, email, datum narození, atd.),
- osobní údaje úřední (rodné číslo, atd.),
- sociální status (rodinná situace, atd.),
- finanční informace (číslo účtu, atd.),
- je možné přidat dodatečné informace pomocí funkce „Další pole“.

## 3 Kategorie subjektů údajů zapojených do zpracování osobních údajů v Kleosu

- Klienti a partneři Správce,
- akcionáři, partneři, zaměstnanci a ostatní personál Správce, včetně stážistů nebo dočasných asistentů, atd.,
- ostatní osoby, jejichž údaje jsou zpracovány Správcem, např. protistrany.

## 4 Účely zpracování

Wolters Kluwer specifikuje, že Kleos je možné použít k následujícím účelům:

- Centralizovaná správa kauz, kontaktů a dokumentů,
- Kleos Connect: zabezpečená výměna dokumentů s vašimi zákazníky a ostatními stranami,
- účetnictví a fakturace: na základě zaznamenaných činností je možné automaticky vytvářet fakturační dokumenty, upomínky nebo vytvářet finanční přehledy,
- propracované možnosti vyhledávání a reportingu,
- export informací do reportů.

## 5 Doba, po kterou budou osobní údaje uloženy

Vy jako Správci si sami určujete dobu uložení údajů o svých klientech (spisy, osobní údaje, dokumenty, atd.).

Wolters Kluwer provádí denní zálohu klientských databází. Tato záloha je uložena 30 dní.

Osobní údaje budou zpracovány a uchovány po následující dobu:

- **Po importu dat z jiného softwaru:** po importu dat z jiného softwaru neuchováváme žádné informace. Správce je sám zodpovědný si tyto informace uložit/zálohovat a v případě potřeby je dát k dispozici Wolters Kluwer.
- **Osobní údaje při vyžádání podpory:** kontakty jsou anonymizovány šest měsíců po ukončení smlouvy. Jako správce máte povinnost ujistit se, že nesdílíte citlivé údaje při požadavku na podporu a řešení požadavku (screenshoty atd.).
- **Kopie vašich dat v souvislosti s požadavkem na podporu:** ve specifických případech pro odhalení technického problému kopírujeme vaši databázi do šifrovaného testovacího prostředí. Data z aktivního prostředí jsou do testovacího přenášena šifrovanou komunikací.
  Pro tento proces potřebujeme vaše svolení. Vaše data jsou použita výhradně k vyřešení problému a ihned potom jsou vymazána.
- **Po vypršení platnosti smlouvy:** data poskytujeme v obecně přístupném formátu. Na našich serverech data uchováváme ještě po dobu tří měsíců.

## 6 Podpora

Pro vyřešení případného problému nebo dodatečného nastavení potřebuje Wolters Kluwer přístup do databáze Správce.

- Správce může dát přístup zaměstnanci Wolters Kluwer aktivováním Uživatele podpory. Správce může tuto funkci kdykoliv vypnout.
- Pokud je třeba přístup k technickým prostředkům Správce, vyžádá si Wolters Kluwer přístup na počítač Správce pomocí sdílení obrazovky. Pro vzdálený přístup je nutná aktivace od Správce. Aktivace se provádí zadáním kódu poskytnutého Wolters Kluwer. Správce je odpovědný za skrytí veškerých citlivých informací před potvrzením vzdáleného přístupu.

## 7 Bezpečnostní opatření

S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provede Wolters Kluwer vhodná technická a organizační opatření, aby zajistil úroveň zabezpečení odpovídající danému riziku.

### PODROBNÁ TECHNOLOGICKÁ A ORGANIZAČNÍ OPATŘENÍ

#### 7.1 Řízení přístupu: budovy

Přístup do budov Wolters Kluwer podléhá technickým i organizačním opatřením: řízení přístupu s personalizovanými čipy, elektronické zámky dveří, zavedené postupy pro návštěvy na recepci.

Správce musí také zajistit, aby byla nastavena odpovídající bezpečnostní opatření ohledně přístupu do jeho budov.

## 7.2 Řízení přístupu: systémy

Jako Zpracovatel vyžaduje Wolters Kluwer povinné autorizace z důvodu přístupu k sítím, operačním systémům, administraci uživatelů a aplikací: pokročilé protokoly hesel, automatické vypršení a blokování nesprávných hesel, individuální účty s uchováváním historie, šifrování, hardwarové a softwarové firewally.

Správce musí zajistit odpovídající bezpečností opatření týkající se jeho hesel a elektronických přístupů.

## 7.3 Řízení přístupu: data

Jako Zpracovatel má Wolters Kluwer přístup k datům řízený interními organizačními opatřeními: administrace uživatelů a uživatelských účtů se specifickým přístupem, personál proškolený s ohledem na zpracování dat a jejich bezpečnost, oddělení aktivních a testovacích systémů, přiřazení specifických práv a ukládání historie používání, přístupů a mazání.

## 7.4 Šifrování dat:

### 7.4.1 Přenos

Přenos dat přes HTTPS je šifrován 2048-bitovým PKI certifikátem a je certifikován společností Norton.

### 7.4.2 Úložiště

Databáze na našich discích šifrujeme specifickým certifikátem / privátním klíčem s použitím algoritmu AES.

## 7.5 Schopnost zajistit neustálou důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování

Řízení přístupu k osobním údajům podléhá vnitřním nařízením, včetně směrnic organizace pro přístup k informacím, zavedení systému administrace uživatelů, šíření povědomí o správě informací a hesel mezi zaměstnanci, řízení síťových přístupů včetně oddělení citlivých sítí a řízení přístupu k operačnímu systému a podpůrným aplikacím. Konkrétní opatření zahrnují:

- Předepsanou/naprogramovanou strukturu autorizací;
- rozlišená přístupová práva (včetně čtení, úprav a mazání);
- definice rolí;
- logování/auditování.

Osobní údaje jsou izolované. Opatření zahrnují:

- oddělení funkcí (aktivní/testovací data);
- oddělení vysoce citlivých dat;
- omezení účelu /rozdělení dle účelu;
- směrnice/opatření pro zajištění oddělených úložišť, úpravy, mazání a přenosu dat.

Od Správce vyžaduje Kleos zadání hesla, které zajistí důvěrnost všech dat zadaných do systému. Kleos také umožňuje spravovat přístupová práva k informacím pro jednotlivé členy kanceláře, pokud to Správce vyžaduje. Správce si pak nastavuje vnitrofiremní pravidla pro důvěrné údaje.

## 7.6 Schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů

Dostupnost dat je nepřetržitě kontrolována síťovým monitorovacím systémem. Pro prevenci ztráty dat jsou prováděny každodenní zálohy dat s přednastavenou platností. Další opatření zahrnují:

- procedury záloh;
- přepěťové ochrany;
- fyzicky oddělené nosiče dat pro zálohy;
- zrcadlení serverových pevných disků (RAID);
- antivirové systémy/filtry spamů/firewall/detekce prolomení systému/plán obnovy při havárii;
- systémy ochrany proti ohni/vodě (včetně hasicích systémů, požárních dveří a detektorů kouře/ohně).

## 7.7 Procesy pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování:

Sytém Kleos je nepřetržitě monitorován:

- V rámci monitoringu 24/7 jsou pečlivě sledovány informace jak o zdraví systému, tak výkonu, a to pro každého klienta individuálně;
- nezávislá externí společnost provádí každoročně testy odolnosti proti vnějšímu průniku;
- navíc je neustále aktivní systém detekce průniků a podává upozornění v reálném čase;
- webová stránka Kleos je také certifikovaná;
- McAfee Security pečlivě monitoruje Kleos každý den;
  - certifikuje, že je webová stránka bezpečná, odolná vůči virům a pokusům o vniknutí a chráněná před útoky hackerů na servery a přenos dat;
  - jsme informováni o jakýchkoliv rizicích v reálném čase, takže můžeme útokům okamžitě zabránit;
- Norton Symantec nepřetržitě monitoruje naše zašifrované přenosy dat pomocí SSL certifikátu;
  - test zranitelnosti se provádí každý měsíc a vždy obdržíme související report.

## 7.8 Dostupné certifikace

Certifikát ISO/IEC 27001