

## OBECNÉ PROHLÁŠENÍ KE KOMPATIBILITĚ PRODUKTŮ SPOLEČNOSTI

### ATLAS CONSULTING SPOL. S R.O. ČLEN SKUPINY ATLAS GROUP

IČO: 465 78 706, SE SÍDLEM VÝSTAVNÍ 292/13,

OSTRAVA – MORAVSKÁ OSTRAVA, 702 00

(DÁLE JEN „ATLAS CONSULTING“)

### S OBECNÝM NAŘÍZENÍM O OCHRANĚ OSOBNÍCH ÚDAJŮ - GDPR

---

#### 1. Obecně

Softwarové produkty společnosti ATLAS consulting jsou plně připravené vyhovět požadavkům jejich zákazníků na ochranu osobních údajů v souvislosti s účinností Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Vzhledem k lišícím se potřebám jednotlivých zákazníků (různý rozsah a množství zpracovávaných osobních údajů, technické zázemí, způsob práce) nabízí softwarové produkty variantní způsoby řešení bezpečnosti zpracovávaných osobních údajů.

Primárním nástrojem těchto řešení je bezesporu možnost správy přístupu více uživatelů pod vlastními přihlašovacími údaji ve všech softwarových produktech. Každý uživatel jednotlivého produktu může mít vlastní přihlašovací údaje a vlastní nastavení práv k činnosti v daném produktu. Umožňuje tak zákazníkovi zvolit způsob práce a schéma ochrany osobních údajů. Ať již přístup všech pracovníků pod jedním uživatelským účtem (např. při velmi malém počtu vzájemně zastupitelných pracovníků a zpracovávání malého objemu osobních údajů s velmi nízkým rizikem pro subjekty údajů), až po zcela individuální řízení přístupu prostřednictvím individuálních uživatelských účtů s individualizovaným nastavením uživatelských oprávnění.

Veškerá data softwarových produktů jsou ukládána šifrovaně do databáze (v případě desktopových produktů je šifrování volitelné) a případně do standardního souborového systému (zejména dokumenty) na úložiště, podle volby zákazníka. Standardizovaný způsob ukládání dat eliminuje rizika ztráty a nekonzistence dat a umožňuje používat další standardní technická bezpečnostní opatření. Umístění databázového a souborového úložiště v případě desktopových produktů stejně jako tato technická bezpečnostní opatření opět volí zákazník v souladu s jeho schématem ochrany osobních údajů s ohledem na to, že k datům lze přistupovat na databázovém a souborovém úložišti bez použití softwarového produktu.

V případě že se pro zákazníka nejeví ochrana osobních údajů jako dostatečná i při provedení veškerých možných bezpečnostních technických a organizačních opatření, společnost ATLAS consulting nabízí možnost ukládání dat svých softwarových produktů v databázi Firebird šifrovaně (např. není-li databázové úložiště pod výlučnou kontrolou zákazníka, nelze zavést bezpečnostní opatření, osobní údaje jsou ukládány ve velkém rozsahu, jsou ukládány citlivé údaje, apod.). V takovém případě jsou v databázi uložená data chráněna i v případě kompromitace databázového úložiště.

## 2. Doporučení pro nejvyšší míru ochrany dat

Aby bylo dosaženo nejvyšší míry ochrany dat (ať již při současném použití šifrovaného ukládání dat, tak i bez něj), společnost ATLAS consulting doporučuje přijmout tato opatření:

- instalovat softwarový produkt v souladu se systémovou příručkou,
- každému jednotlivému uživateli softwarového produktu přidělit jeden uživatelský účet chráněný heslem,
- zavést opatření pro bezpečné nakládání s hesly, zejména pravidla pro tvorbu bezpečného hesla a pro jejich bezpečné používání (minimální délka hesla, zákaz slovníkových hesel, požadavky na speciální znaky, povinnost obnovy hesla, ochrana hesla uživatelem, apod.),
- zavést opatření pro bezpečnou práci se softwarovým produktem a jeho daty (povinnost odhlášení ze softwarového produktu, popř. zařízení při přerušení nebo ukončení práce, neumožnění přístupu do softwarového produktu osobě odlišné od přihlášeného uživatele, zákaz exportu dat, povinnost pravidelných záloh dat, apod.),
- zavést opatření pro bezpečnou práci s výpočetní technikou (ochrana fyzického přístupu k technickým prostředkům neoprávněnou osobou, vhodná politika uživatelských účtů, šifrování disků u přenosných zařízení, zákaz zanechání přenosných zařízení bez fyzické kontroly mimo chráněné objekty, neumožnění přístupu nepřihlášené osoby, vhodné zálohování, ochrana proti virům a jinému malware, apod.),
- zavést opatření pro omezení přístupu k úložištím pouze pro oprávněné osoby (a to jak fyzického, tak elektronického, obvykle pouze pro správce IT, zpřístupnit komunikační port databázového systému pouze pro uživatelské počítače),
- dostatečně seznámit všechny uživatele, vč. správců IT se zavedenými organizačními bezpečnostními opatřeními (interní směrnice, školení, apod.),
- dostatečně vymáhat dodržování organizačních bezpečnostních opatření (kontrola dodržování, úprava opatření při zjištění nedostatku, sankcionování porušení, apod.).

## 3. Podrobněji k šifrování dat

Komunikace mezi uživatelskou aplikací a databázovým serverem je vždy šifrována. Jestliže zákazník zavede možnost ukládání dat svých softwarových produktů v databázi Firebird šifrovaně, budou data v databázi ukládána šifrovaně. V případě kompromitace komunikace mezi klientskou aplikací a serverem nebo kompromitace databáze tak nedojde ke kompromitaci přenášených a ukládaných dat.

Pro šifrování softwarové produkty používají 128 bitový kryptovací klíč. Pro jeho předávání uživatelům za účelem přístupu do databáze existuje u desktopových produktů několik metod použitelných v závislosti na potřebách jednotlivých zákazníků. Stejně tak existuje několik standardních metod pro jeho uložení a používání (uvedených v systémové příručce). Vedle toho společnost ATLAS consulting nabízí individuální návrh a realizaci řešení tohoto opatření podle individuálních potřeb zákazníka.

Zavedení možnosti ukládání dat svých softwarových produktů v databázi Firebird šifrovaně doporučujeme tam, kde zákazník požaduje zvýšit ochranu proti neoprávněnému přístupu k datům (a jejich následnému neoprávněnému získání a zneužití) pro případ nemožnosti nebo nedostatečnosti zavedení jiných bezpečnostních opatření. K neoprávněnému přístupu k datům může dojít jednak interně, tj. osobou, která má oprávněný přístup k databázovému úložišti, a jednak externě, tj. osobou, která si zjedná k databázovému úložišti neoprávněný přístup (např. hacking, získání přístupových údajů oprávněné osoby, krádež fyzických médií vč. serveru, notebooku, apod.).

Data ukládaná v souborech v běžném souborovém systému (tedy zejména dokumenty formátu word, excel, pdf, apod.) nejsou ukládána šifrovaně, neboť s nimi uživatel pracuje i mimo softwarový produkt společnosti ATLAS consulting. Ochranu souborového systému (která může zahrnovat také jeho šifrování) tedy zavádí podle svých potřeb zákazník (s ohledem na druh, objem, rozsah a povahu osobních údajů, které jsou v souborech ukládány).

Možnost ukládání dat svých softwarových produktů v databázi Firebird šifrovaně existuje pro tyto desktopové aplikace:

- Advokátní spis
- Smlouvy+
- Manažer datových schránek
- Kontrola insolvence
- Manažer Smluv a Dokumentů
- Manažer Smluv a Dokumentů Cloud

Data jsou automaticky ukládána šifrovaně v těchto online aplikacích:

- CODEXIS GREEN
- Manažer Datových Schránek Online
- Chytrá Datovka
- Právní Výpočty
- Hlídač Ochranných Známek
- Právní Prostor / Právní Poradna
- CODEXDATA

**ATLAS consulting spol. s r.o.**  
IČO: 465 78 706  
Výstavní 292/13, Ostrava – Moravská Ostrava  
702 00

Platnost ke dni 20. 9. 2021