

Vyjádření k ochraně osobních údajů GDPR uložených v programu Wintropos

24.5.2018

Zabezpečení osobních údajů pacientů uchovávaných v programu Wintropos

Program Wintropos (dále pouze „program“, nebo „Wintropos“) je lékařský software určený pro zdravotnická zařízení, který slouží k vedení zdravotní dokumentace o pacientech, vyúčtování zdravotní péče zdravotním pojišťovnám, vydávání lékařských předpisů a dalším úkonům souvisejícím s administrativou ve zdravotnických zařízeních. Nakládání s těmito daty je v České republice a celé EU nově upraveno nařízením Evropského parlamentu a Rady 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů, označovaném zkratkou GDPR (General Data Protection Regulation).

V programu Wintropos jsou typicky uchovávány a zpracovávány osobní údaje pacientů, jejich kontaktní údaje, informace o jejich zdravotním stavu (včetně rodinné a sociální anamnézy, v případě potřeby etnický původ a genetické údaje) a to za účelem řádného vedení zdravotnické dokumentace k poskytované zdravotní péči a plnění povinností při poskytování zdravotních služeb a případně i další informace.

Zdravotní údaje jsou dle GDPR speciální kategorií osobních údajů a zasluhují vyšší stupeň ochrany. Tvůrci programu Wintropos si byli (na rozdíl od většiny konkurentů) od počátku vědomi citlivosti zdravotních záznamů ukládaných v databázi programu. Aby se zamezilo možnému zneužití těchto údajů neoprávněnými osobami (např. v případě neoprávněného zkopírování databáze, zálohy dat a podobně), byly a jsou databáze v programu Wintropos šifrované a zabezpečené moderními principy tak, aby nebylo možné jejich přečtení mimo program Wintropos.

Od verze programu 1.6.0 je navíc pro zvýšení ochrany do programu Wintropos zavedena povinnost nastavit si a používat heslo, bez kterého program nebude možné spustit. Věříme, že toto opatření dále přispěje ke zvýšení bezpečnosti uchovávaných dat (např. v případě krádeže počítače včetně licencovaného programu Wintropos).

Veškeré údaje do programu Wintropos zadává uživatel (personál zdravotnického zařízení), údaje nejsou generovány ani načítány automaticky. Za zákonnost zpracování těchto údajů zodpovídá uživatel, resp. správce osobních údajů v rámci daného zdravotnického zařízení. Ten je také povinen zvážit, které údaje je oprávněn evidovat a které ne.

Další úroveň zabezpečení (z nichž lze jmenovat např. ochranu počítače s uloženými daty heslem, natočení monitoru tak, aby nebylo možné data neoprávněně přečíst, instalace a pravidelné aktualizace antivirového programu i operačního systému, případně šifrování obsahu pevného disku, ochrana proti neoprávněnému vniknutí do ordinace atd.) je pak v režii a zodpovědnosti jednotlivých uživatelů.

Přenosy dat v programu Wintropos

Zdravotnický program Wintropos neodesílá svévolně (bez přímého pokynu uživatele) žádná data na webové servery ani další zařízení mimo zdravotnické zařízení uživatele. Všechna v programu zadaná data jsou uložena na lokálním pevném disku uživatele. Jakákoliv manipulace s těmito daty je tedy

plně v režii uživatele. Program Wintropos nepodporuje vzdálenou správu, tvůrci programu ani další osoby nemají k datům uloženým uživateli přístup.

V programu je dále možné provádět export záznamů o provedených zdravotních výkonech do textového souboru (vytváření dávek pro pojišťovnu). Wintropos umožňuje přenos dávek dokladů přímo z programu na servery zdravotních pojišťoven. Tento přenos dat zabezpečen a splňuje požadavky současné legislativy. Za zabezpečení exportovaných dat při jakékoliv jiné manipulaci s nimi odpovídá uživatel programu, který úkon provádí. Totéž platí i pro uchovávání exportovaných (nešifrovaných) dat.

Obecně nedoporučujeme posílat jakákoliv nešifrovaná osobní nebo jinak citlivá data emailem, ani přes další komunikační programy (např. Messenger, Skype, WhatsApp) nebo sociální sítě, kde není možné zaručit, že data nemohou být zobrazena třetí stranou. Zrovna tak nedoporučujeme nezabezpečená data nosit na přenosných pamětech (USB flash), které lze snadno ztratit. Data na paměťových médiích určených k přenášení by měla být vždy řádně zabezpečena (šifrování, archivace s heslem a podobně)!

Obecné informace o nařízení o ochraně osobních údajů (GDPR) ve zdravotnictví jsou k dispozici např. na webu České lékařské komory, podrobněji je pak metodika zavedení GDPR do lékařské praxe zpracována na stránkách ministerstva zdravotnictví:

[https://www.lkcr.cz/gdpr-448.html?do\[loadData\]=1&itemKey=cz_1](https://www.lkcr.cz/gdpr-448.html?do[loadData]=1&itemKey=cz_1)

https://www.mzcr.cz/Legislativa/obsah/implementace-gdpr_3805_11.html