18. 12. 2025

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

# Využívání nástrojů umělé inteligence: proč je GDPR relevantní?

Nasazení nástrojů umělé inteligence (AI) již dávno není doménou technologických firem. Umělou inteligenci dnes využívají zdravotnická zařízení, právníci, marketingové agentury, banky, výrobní podniky, ale i mnoho dalších typů organizací vč. veřejných institucí. Většina těchto organizací přitom AI sama nevyvíjí, ale v pozici (terminologií AI Aktu) „zavádějících subjektů" využívá již hotová řešení třetích stran.

Spolu s tím však musí řešit důležitou otázku, jakou mohou mít odpovědnost za zpracování osobních údajů ve fázi tréninku AI, kterou pak v postavení zákazníka využívají? A jak se GDPR uplatní na fázi nasazení AI a jejího následného používání?

První otázkou, tedy možnou odpovědností za protiprávní trénink umělé inteligence na osobních údajích, jsme se zabývali v předchozích třech článcích[1], které obsahují i naše doporučení pro snížení případných GDPR rizik. V této navazující sérii článků si tato doporučení nejprve stručně připomeneme, protože zákonnost trénování modelu, resp. nástroje, nebo alespoň adekvátně snížená rizika z případné nezákonnosti, jsou prvním předpokladem jeho nasazení.

Následně v tomto a dalších čtyřech článcích postupně vysvětlíme, proč a kdy je GDPR relevantní i pro nasazení a používání nástrojů AI, co by měly zavádějící subjekty při takovém nasazení a používání zvážit, a jak by se u daného nástroje měly vypořádat s celkovou GDPR compliance.

## (Ne)legálnost tréninku AI z pohledu GDPR a snížení rizik

Každé zavedení nástroje umělé inteligence začíná otázkou, zda model, resp. nástroj vůbec vznikl „v souladu se zákonem". Společnost, která AI využívá, obvykle nemá možnost ovlivnit způsob, jakým byla umělá inteligence natrénována. Případné porušení GDPR ve fázi vývoje modelu může založit i odpovědnost zavádějícího subjektu, tedy organizace, která tento model sama nevyvíjí, ale pouze využívá. Evropský sbor pro ochranu osobních údajů (EDPB) na této samostatné odpovědnosti zavádějícího subjektu založil svá doporučení ve stanovisku 28/2024, z něhož je zřejmé, že se jí nelze vyhnout pouhým odkazem na neprověřená marketingová tvrzení poskytovatele. Naopak, zavádějící subjekt by měl provést vlastní „prověrku" daného nástroje (vč. dodržení GDPR při vývoji modelu), přičemž hloubka této kontroly se odvíjí od rizikovosti daného modelu či nástroje.

Základní otázkou, kterou by si měla každá organizace zavádějící AI položit, je, zda byl zaváděný model či nástroj vyvinut (trénován) na datech, která obsahovala osobní údaje. Pokud nebyl, GDPR se na daný model a jeho trénink vůbec nevztahuje. Stejně tak platí, že se GDPR na daný model nevztahuje v případě, kdy byl model sice trénován na osobních údajích, ale následně byl anonymizován do té míry, že z něj nelze přímo (např. útokem na model) nebo nepřímo (např. přes prompt uživatele) osobní údaje extrahovat. Správně provedená anonymizace modelu může dokonce zavádějící subjekt zbavit odpovědnosti za užívání modelu i v případě, že před provedením anonymizace modelu došlo při jeho vývoji k porušení GDPR.Pokud daný model na osobních údajích trénován byl a data nebyla anonymizována, GDPR se na takové zpracování uplatní, vč. požadavku na právní titul pro toto zpracování – nejčastěji oprávněný zájem podle čl. 6 odst. 1 písm. f) GDPR,

doplněný o tříkrokový test proporcionality, nebo výjimečně souhlas dotčené osoby podle písm. a) GDPR. Tam, kde se využívají zvláštní kategorie údajů (například zdravotní nebo biometrické informace), je situace ještě složitější. Čl. 9 GDPR stanoví velmi úzký okruh výjimek připouštějících zpracování této kategorie dat a jejich naplnění bývá v praxi obtížné.

## Doporučení ke snížení rizik odpovědnosti za nezákonnost tréninku AI

Co může organizace zavádějící nástroje umělé inteligence udělat proto, aby snížila rizika odpovědnosti za protiprávní využití osobních údajů k tréninku daného AI nástroje?

Zjednodušeně řečeno, měla by ověřit nástroj, který hodlá implementovat, v rozsahu odpovídajícím jeho rizikovosti pro dotčené osoby i pro organizaci jako takovou. Toto prověření by se dle okolností (a nad rámec základního ověření důvěryhodnosti daného dodavatele a neexistence negativních regulatorních rozhodnutí) mělo zaměřit na to, zda:

- při trénování a dalším vývoji AI nebyly využity osobní údaje, případně vč. vyžádání informací o použitých tréninkových datech, aby prohlášení dodavatele mohla ověřit
- byl model, resp. nástroj AI, který byl trénován na osobních údajích, správně anonymizován a osobní údaje z něj nelze přímo ani nepřímo extrahovat, včetně případně vyžádání informací o tréninkových datech, použité technologii anonymizace a opatření zabraňující přímé a nepřímé extrakci osobních údajů, které organizace může v relevantních případech i sama otestovat
- dodavatel, resp. vývojář neanonymizovaného modelu ve fázi vývoje splnil požadavky GDPR, zejména existence titulu pro dané zpracování, informování subjektů údajů apod., případně včetně vyžádání a ověření balančního testu a prokázání dodržení transparentnosti ve fázi vývoje.

## Relevance GDPR při nasazení a používání nástrojů AI

Řada společností se domnívá, že ověřením legality vývoje AI nástroje jejich GDPR povinnosti končí. Opak je pravdou. Dosud popisované kroky mají za cíl snížit potenciální rizika nepřímé odpovědnosti vyplývající z porušení GDPR, kterého se ve fázi učení mohla dopustit třetí strana (vývojář, resp. dodavatel AI nástroje).

Nicméně, z pohledu možné přímé odpovědnosti je to právě fáze nasazování a používání AI, ve které často dochází ke zpracování osobních údajů v rozsahu, který je z pohledu regulace (a možné odpovědnosti zavádějícího subjektu) zásadní.

## Typické zpracování osobních údajů

Jaké jsou typické situace, resp. kategorie činností, kdy organizace pomocí AI zpracovávají osobní údaje?

První typickou situací je proces primárně zaměřený na zpracování osobních údajů, který je zajištěný nebo podporovaný AI. Může se jednat jak o zpracování většího množství dat, tak i řešení individuálních případů. Příkladem rozsáhlejšího zpracování dat může být např. analýza a segmentace klientských databází, hodnocení či třídění zaměstnanců podle určitých kritérií, vyhledávání specifických skupin osob ve větší evidenci podle stanovených klíčů atd. Individuálním případem pak může být např. vyhodnocení životopisu uchazeče o zaměstnání, posouzení žádosti o finanční produkt, žádosti o sociální dávku, analýza zdravotnických informací nebo snímků z vyšetření u

specializovaného lékaře atd.

Druhou kategorií je situace, kdy je AI využívána k řešení úkolu či zadání, které osobní údaje obvykle obsahují, byť zpracování těchto dat není primárně cílem. Příkladem může být řešení alertů z bezpečnostních a monitorovacích nástrojů, řešení kyberbezpečnostních incidentů, analýza dokumentace, která může obsahovat osobní údaje, např. smlouvy, klientské či zaměstnanecké dokumentace atd.

Třetí kategorií je situace, kdy využívaný nástroj umělé inteligence s osobními údaji pracuje jen v některých případech, nikoliv pravidelně, nebo jen jako nepřímý důsledek či součást hlavního úkolu, který umělá inteligence plní. Jedná se například o analýzu či hodnocení činnosti informačních systémů nebo výrobních prostředků, kdy zpracovávané a hodnocené informace mohou obsahovat rovněž informace o konkrétních lidech, ač to není primárním cílem.

Další kategorií mohou být situace, kdy jsou dále využívána data ze samotné interakce (lidského) uživatele s AI. Ať už jeho aktivita, zadávání promptů, jejich obsah a reakce AI nástroje, ale i logy či další záznamy o aktivitě uživatelů. Tyto informace jsou v praxi dále využívány typicky k rozvoji modelu či nástroje umělé inteligence, zajištění jeho dostupnosti, stability, bezpečnosti atd.

Specifickou situací pak je, když je AI nástroj integrován na další systém uchovávající nebo zpracovávající osobní údaje v organizaci, např. CRM, HR systémy atd., a získá díky tomu přístup k osobním údajům ve velkém rozsahu, byť jejich zpracování primárně není jeho cílem. Ochranu osobních údajů je ale i v tomto případě nutné řešit.

## Rizika AI z pohledu osobních údajů

Využití AI v praxi již přináší řadu výhod, úspor a nových možností. Nástroje umělé inteligence s sebou však nesou i jistá specifická rizika. Řada z nich se dotýká i ochrany osobních údajů a plnění dalších povinností podle GDPR.

Mezi typická rizika, která by měl každý zavádějící subjekt - správce osobních údajů v přiměřeném rozsahu řešit, lze podle našeho názoru zařadit především tato:

- Ztráta kontroly nad osobními údaji. Pokud AI nástroj pracuje s osobními údaji, hrozí, že se osobní údaje dostanou mimo kontrolu správce - zavádějícího subjektu. Poskytovatelé nástrojů totiž často využívají jazykové modely či další podpůrné technické nástroje od dalších poskytovatelů, se kterými mohou v řadě případů vstupy od koncových uživatelů sdílet. Stejně tak hrozí, že tyto údaje mohou být úmyslně či v důsledku nedostatečného zabezpečení sdílené s dalšími klienty poskytovatele, nebo získány neoprávněnou třetí stranou, např. technikou tzv. *prompt injection*.
- Přenosy osobních údajů mimo EU bez dostatečných záruk. Při předávání osobních údajů mimo Evropskou unii, včetně jejich zpřístupnění poskytovateli AI, je správce povinen přijmout opatření pro zajištění dostatečné ochrany práv dotčených osob. GDPR těchto opatření nabízí celou řadu: Některé země svým právním prostředím zaručují srovnatelnou míru ochrany a Komise je proto označí za tzv. Bezpečné země, do kterých lze osobní údaje předávat bez dalšího (např. Velká Británie, Švýcarsko, Jižní Korea, Japonsko atd.[2]). U ostatních se v praxi nejčastěji využívají tzv. Standardní smluvní doložky dle vzoru prováděcího rozhodnutí Komise 2021/914[3], které mají smluvně garantovat, že zpracovatel sídlící v zemi, která srovnatelnou míru ochrany nezaručuje, sám od sebe podnikne takové kroky, aby se míra ochrany subjektu údajů nesnížila. Správce je každopádně odpovědný za to, aby před využitím AI nástroje jednoznačně určil, zda osobní údaje mohou při jeho využití opustit hranice EU a pokud ano, zavést dostatečná bezpečnostní opatření.

- Nedostatečná transparentnost zpracování. Řada běžně dostupných AI nástrojů využívá dílčí dodavatele či nástroje od jiných subjektů. Obvykle se jedná o velké jazykové modely, dílčí ICT nástroje a služby pro zajištění funkčnosti, dostupnosti a bezpečnosti AI nástroje atd. Pro správce je důležité tento možný datový tok zmapovat a subjekty údajů o něm informovat, aby mohly reálně vykonávat svá práva dle GDPR.
- Dalším rizikem je rovněž ztížená možnost některá práva subjektu údajů reálně vykonat. Typickým případem je zahrnutí osobního údaje, byť v pseudonymizované či jinak chráněné podobě, do modelu, který je využíván pro poskytování služby, nebo jeho uchování v logu. Pokud dotčená osoba požádá například o kompletní přístup k těmto osobním údajům, o jejich opravu (pokud je údaj nepřesný nebo neaktuální) nebo výmaz, v praxi to půjde často realizovat jen obtížně.

## Shrnutí a doporučení

Jak jsme uvedli výše a detailněji rozebrali v našich předchozích článcích, zavádějící subjekt může být (spolu)odpovědný za případné nezákonnosti zpracování osobních údajů při vývoji jím využívané AI. Za účelem snížení rizik z toho vyplývajících doporučujeme (souladně s doporučeními EDPB), aby zavádějící subjekty prováděly prověrky AI nástrojů, a to dle rizikovosti daného AI nástroje pro subjekty údajů, ale také pro danou zavádějící organizaci jako takovou.

Ověření legality vývoje AI nástroje je nicméně krokem nezbytným, nikoliv jediným. V navazující fázi nasazení a používání AI totiž často dochází ke zpracování osobních údajů způsobem a v rozsahu, který je z pohledu regulace (a možné odpovědnosti zavádějícího subjektu) ještě důležitější. A v tomto případě již leží plné břímě souvisejících rizik, povinností a možných (přímých) odpovědností právě na zavádějícím subjektu.

Mezi tato rizika patří mimo jiné tzv. function creep neboli využití nástroje (a tedy i osobních údajů) za jiným než původně zvažovaným a deklarovaným účelem, nesprávné stanovení právního titulu a tím celková nezákonnost zpracování dat, nedostatečná transparentnost, ztížení či nemožnost výkonu některých práv subjektů údajů, ztráta kontroly nad osobními údaji, nebo rizika týkající se předávání osobních údajů do třetích zemí.

V dalších článcích této série se na některá tato rizika podíváme blíže a rozebereme, jak konkrétně by dle našeho názoru měly zavádějící subjekty k plnění svých GDPR povinností přistoupit.

**Mgr. František Nonnemann,**
konzultant pro oblast ochrany dat, compliance, řízení rizik a AI

**Mgr. Michal Nulíček, LL.M., FCIArb**,
advokát a partner ROWAN LEGAL, odborník na ochranu osobních údajů a regulace

ROWAN LEGAL, advokátní kancelář s.r.o.

GEMINI Center
Na Pankráci 1683/127
140 00  Praha 4

Tel.:  +420 224 216 212
Fax:  +420 224 215 823
e-mail:  praha@rowan.legal

---

[1] K dispozici >>>zde, zde a zde.

[2] Seznam těchto bezpečných třetích zemí je k dispozici na webových stránkách Komise: K dispozici >>> zde.

[3] Prováděcí rozhodnutí Komise (EU) 2021/914 ze dne 4. června 2021 o standardních smluvních doložkách pro předávání osobních údajů do třetích zemí podle nařízení Evropského parlamentu a Rady (EU) 2016/679.



## Další články:

- Dokazování negativních skutečností ve sporném řízení
- Neoprávněný odběr elektřiny – překvapení vlastníka?
- Rodič u dítěte v nemocnici: právo na přítomnost neznamená bez dalšího právo na přespání na jip/jirp

- Pokuta za švarcsystém kurýrů Rohlíku potvrzena Ústavním soudem
- Metropolitní plán schválen. Je Váš projekt v bezpečí?
- Posouzení shody dle AI Act - zkušenosti z praxe
- Začínají soudy zohledňovat náklady podnikatelů při plnění právních povinností v oblasti e-commerce?
- Byznys a paragrafy, díl 35: Ručení za dluhy z podnikání u OSVČ a s.r.o.
- Bezpilotní systémy vlastní konstrukce v kategorii Specific: regulatorní požadavky a praktické aspekty
- Nefungující rozsah péče o dítě. Cesta přes využití terapie a dalších opatření podle ustanovení § 503 zákona o zvláštních řízeních soudních
- De iure traktor, de facto nákladní vozidlo, už ne tolik výhodná dualita