

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

Jak vytrénovat umělou inteligenci na veřejně dostupných datech? 2. díl: Oprávněný zájem jako titul pro trénink AI

V prvním díle* našeho seriálu o tréninku AI nástrojů na veřejných datech jsme si podrobně rozebrali základní principy GDPR, které se uplatní na neanonymizovaná osobní data, která jsou využívána k tréninku AI. Nyní je čas zaměřit se na právní tituly, které umožňují zpracování osobních údajů, včetně veřejně dostupných dat. Konkrétně na ten nejvýznamnější. Oprávněný zájem hraje klíčovou roli nejen ve fázi vývoje AI, ale i v okamžiku, kdy se nástroj začne používat v praxi. Co obnáší třístupňový balanční test? Jak vyhodnotit přiměřenost a závažnost zájmu správce a zásahu do práv dotčených osob? V tomto díle si rozebereme jeden z nejčastěji využívaných právních základů v technologickém světě.

Oprávněný zájem je v praxi jedním z nejpoužívanějších, ne-li nejpoužívanějším právním titulem i mimo oblast AI. I z toho důvodu vydal EDPB návrh vodítek, která se jeho využitím v praxi zabývají.^[1] V rámci těchto vodítek EDPB formuloval třístupňový test, kterým musí využití oprávněného zájmu projít a který se uplatní i na posouzení vhodnosti oprávněného zájmu pro trénink AI.

Ve svém novém Stanovisku ke zpracování osobních údajů v kontextu AI^[2] Evropský sbor využití oprávněného zájmu v kontextu vývoje AI nevyloučil. Naopak se dá říci, že jeho aplikaci výslovně připustil – to ovšem za předpokladu, že budou v kontextu vývoje AI splněny podmínky právě onoho třístupňového testu. Ten EDPB znovu zopakoval a vyložil právě ve vztahu k vývoji AI.

Zákonnost zpracování osobních údajů musí zajistit primárně ten, kdo danou AI vyvíjí. Nicméně, jak si později ukážeme, tato otázka může být relevantní i pro subjekt, který danou AI zavádí, tedy typicky organizace, která si pořizuje AI nástroj dodaný třetí stranou. Ta totiž bude muset před jejím nasazením v určité míře zákonnost zpracování při vývoji ověřit. Domníváme se proto, že je na místě shrnout ony „tři kroky testu“ posouzení oprávněného zájmu.

Balanční test

1. Krok první: Identifikace účelu

V prvním kroku tento test vyžaduje identifikaci jasně vyjádřeného, skutečného a zákonného oprávněného zájmu. Takovým zájmem (účelem) může být např. trénink AI pro lepší hodnocení kandidátů o zaměstnání.

2. Krok druhý: Způsob zpracování údajů a jejich minimalizace

V druhém kroku se posuzuje nezbytnost zpracování pro daný účel a konkrétně zejména to, zda daná činnost zpracování umožní dosažení stanoveného účelu. V případě tréninku AI by se tedy například posuzovalo, zda trénink AI na určitých datech může skutečně zásadním způsobem přispět k vývoji

daného nástroje a zda není reálně dostupný jiný, do soukromí méně zasahující způsob, jak dosáhnout stejného účelu. V našem příkladu by bylo posuzováno například to, zda neexistuje možnost vyvinout jiný nástroj AI pro nábor, který při vývoji nevyžaduje zpracování osobních údajů – zda lze například využít údaje anonymní apod.

Součástí těchto posouzení je také otázka minimalizace údajů, tedy to, zda jsou pro daný účel (trénování AI) využity osobní údaje pouze v minimálním nezbytném rozsahu, resp. zda z tréninkového datového setu nelze některá data vyjmout a pro tento účel je nezpracovávat. V neposlední řadě se v rámci testu nezbytnosti zkoumají také kontext daného zpracování a uplatnění dodatečných záruk a opatření (např. pseudonymizace, která může ztížit identifikaci daného subjektu údajů a tím i podstatně snížit související rizika).

3. Krok třetí: Test vyváženosti

Posledním krokem je test vyváženosti, tedy posouzení toho, zda nad identifikovaným zájmem správce (zde vývojáře AI pro nábor) nepřeváží základní práva, svobody a oprávněné zájmy subjektů údajů. V souvislosti s vývojem AI mohou mezi zájmy subjektu patřit například zájem na sebeurčení a zachování kontroly nad vlastními osobními údaji, mezi ohrožená práva mohou patřit např. právo na soukromý a rodinný život (zejména v případě, kdy „scraping“ dat je prováděn bez vědomí subjektu údajů). Každopádně platí, že v rámci posuzování vyváženosti je vhodné identifikovat a případně i zohlednit možné přínosy pro zájmy a práva subjektu (např. posílení práva na duševní nedotknutelnost při vývoji modelu na identifikaci škodlivého obsahu na internetu).

V rámci testu vyváženosti se také zkoumají přiměřená očekávání subjektů. Dle EDPB jsou očekávání subjektů klíčová zejména s ohledem na celkovou složitost technologie AI. Proto je očekáváním subjektů třeba věnovat dostatečnou pozornost a zajistit např. opravdovou informovanost a pochopení na straně subjektů. Důležitý je ale i širší kontext zpracování včetně toho, zda mezi správcem (zde vývojářem AI) a subjektem údajů existuje nějaký vztah, zda jsou pro trénink AI zpracovávány jen veřejně dostupné údaje, jaká je povaha služby a zdrojů, z nichž byly údaje shromážděny, potenciální další využití daného modelu či nástroje apod.

Zvláštní kategorie osobních údajů

Situace je komplikovanější v případě zpracování citlivých osobních údajů (např. údajů o zdravotním stavu), jejichž zpracování je v čl. 9 GDPR obecně zakázáno, ledaže správce svědčí některá z úzce koncipovaných výjimek.

Aniž bychom se specifické oblasti zpracování citlivých údajů v rámci vývoje AI chtěli věnovat detailně (přičemž stanovisko EDPB se této kategorii údajů nevěnuje vůbec, resp. tuto otázku ze svého posouzení výslovně vylučuje), pouze zmíníme, že jistou naději pro jejich zpracování při vývoji AI může skýtat zejména výjimka pro zpracování zjevně zveřejněných údajů (čl. 9 odst. 2 písm. e) GDPR) nebo zpracování pro vědecké výzkumy a statistické účely (písm. j) stejného ustanovení GDPR), ale jedná se o tak komplexní problematiku, že jí ponecháváme na některý z našich dalších příspěvků.

Jak bezpečně využít neanonymní AI nástroje

V případě, že dodavatel tvrdí, že během tréninku AI nástroje byly použity osobní údaje a tento model nebyl anonymizován, může být subjekt zavádějící daný nástroj (který obsahuje tréninková data) v závislosti na okolnostech teoreticky spoluodpovědný za porušení GDPR, kterého se dodavatel dopustil v rámci vývoje, ať již bude důvodem takové odpovědnosti společné správcovství, nebo bude jeho odpovědnost dovozena jinak.

Jak snížit rizika při využití AI třetích stran

V souladu se stanoviskem EDPB[3] v takovém případě doporučujeme především prověřit splnění požadavků GDPR ve fázi vývoje AI. Míra detailu prověření se bude lišit v závislosti na vyhodnocení rizikovosti daného AI systému, nicméně zásadním se jeví ověření zákonnosti tohoto zpracování a správnosti zvoleného právního titulu. V tomto ohledu EDPB (dle našeho názoru správně) konstatuje, že se nelze spolehnout na prohlášení samotným dodavatelem, byť bude obsaženo např. v EU prohlášení o shodě, které vyžaduje AI Act pro vysoce rizikové AI systémy.

Co konkrétně by tedy měl zavádějící subjekt zkoumat? Vždy minimálně to, jaká tréninková data byla využita, zda nepocházejí ze zjevně nelegálních zdrojů (např. z kybernetického útoku) a zda vůči danému dodavateli, případně jeho nástroji, již nekonstatoval porušení právních pravidel pro ochranu osobních údajů některý dozorový orgán či soud. Míra nezbytného ověření se bude lišit případ od případu a existuje riziko, že toto „základní“ ověření nebude dozorovým úřadům stačit, zejména při vysoce rizikovém využití AI, které představuje významné riziko pro práva a svobody dotčených lidí. Proto je vhodné zvážit i vlastní zjednodušené posouzení zákonnosti zpracování při tréninku daného AI nástroje na základě podkladů a dokumentace ze strany dodavatele.

Správné posouzení oprávněného zájmu je zcela zásadní součástí procesu, kterou by firmy ani dodavatelé neměli podcenit. Jinak jim hrozí, že budou využívat osobní údaje v rozporu s GDPR a jejich produkt či interní proces jim místo zisku či úspor přinese jen riziko vysoké pokuty. Porušení pravidel pro využití osobních dat může způsobit i nesoulad s novým zastřešujícím legislativním rámcem na úrovni EU, tzv. AI Actem. Ten přináší řadu povinností, ale také změnu paradigmatu, v jehož intencích je potřeba o ochraně osobních údajů při využití AI přemýšlet. V závěrečném díle seriálu se proto zaměříme na to, co nová pravidla znamenají v praxi. Nejde totiž jen o nové požadavky na dokumentaci a testování – mnoho subjektů bude muset dle nových pravidel sladit i svoje compliance procesy.



Mgr. František Nonnemann,

vedoucí oddělení Compliance a oddělení Řízení operačního rizika ve společnosti Partners Banka



Mgr. Michal Nulíček, LL.M., FCI Arb,

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: paha@rowan.legal

*Jak vytrénovat umělou inteligenci na veřejně dostupných datech? 1. díl: GDPR, anonymita a odpovědnost uživatele, dostupné na www, k dispozici >>> [zde](#).

[1] Návrh vodítek EDPB č. 1/2024 ke zpracování osobních údajů založeném na čl. 6 odst. 1 písm. f) GDPR. Návrh vodítek byl předmětem veřejné konzultace, ke dni dokončení tohoto článku není k dispozici finální verze. Návrh vodítek je >>> [zde](#).

[2] Stanovisko EDPB 28/24 k určitým aspektům ochrany osobních údajů v souvislosti se zpracováním osobních údajů v kontextu modelů umělé inteligence.

[3] Viz Stanovisko EDPB 28/24 k určitým aspektům ochrany osobních údajů v souvislosti se zpracováním osobních údajů v kontextu modelů umělé inteligence, zejm. kapitola 3.4 a podkapitola 3.4.2 tohoto stanoviska, konkrétně zejména body 129 a násl.

© EPRAVO.CZ - Sběrka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [Hmotněprávní opatrovník obchodní korporace: mezi efektivní ochranou a zásahem do korporační autonomie](#)
- [Byznys a paragrafy, díl 32.: Konkurenční doložka](#)
- [Skryté ujednání v realitní smlouvě - zbytečná hra na schovávanou](#)
- [Odpovědnost člena voleného orgánu dle § 159 OZ a vymezení škody způsobené právnícké osobě](#)
- [Vnosy do společného jmění manželů a jejich valorizace v aktuální judikatuře Nejvyššího soudu a Ústavního soudu](#)
- [Právo na přístup ke kamerovým záznamům: střet GDPR, informačního zákona a praxe veřejných institucí](#)
- [Postoupení pohledávky na výživné jako novinka právní úpravy účinné od 1. 1. 2026](#)
- [Jak zahájit provoz mezinárodní letecké linky do České republiky \(EU\): právní požadavky pro](#)

aerolinky ze třetích zemí

- Mimořádné vydržení a vývoj judikatury Nejvyššího soudu
- Preventivně-sankční funkce náhrady nemajetkové újmy za porušení osobnostních práv pohledem Ústavního soudu
- Odštěpný závod zahraniční společnosti optikou NIS2: Jak správně určit velikost podniku?