2. 7. 2025

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

Právo a umělé inteligence: AI Act, osobní údaje, kyberbezpečnost a další regulace

Požadavky na zpracování osobních údajů v členských státech Evropské unie patří momentálně k těm nejpřísnějším na světě. Hlavním pramenem práva v této oblasti je obecné nařízení o ochraně osobních údajů (GDPR)[1]. Právě díky tomu je v rámci EU zaručen také volný pohyb osobních údajů, který nesmí být nijak omezován ani zakazován. Podmínkou však zůstává, že správce osobních údajů musí mít pro předání dat dalšímu správci právní důvod (titul).

Využívání umělé inteligence[1] je dnes jasným trendem. Umělou inteligenci dnes nasazuje, nebo o tom alespoň plamenně hovoří, řada společností, státních úřadů i samosprávných celků. Stejně tak se vynořila řada nových produktů a dodavatelů, kteří nabízejí AI produkty, služby a nástroje. O dodavatelích, kteří na svůj produkt pouze „přilepili cedulku AI“, aniž by změnili podstatu jejího fungování, ani nemluvě.

Každá organizace, která vyvíjí nebo v praxi zavádí a využívá systémy umělé inteligence, by si měla být vědoma svých právních povinností. Regulace umělé inteligence se přitom neomezuje pouze na Akt o umělé inteligenci[2]. Podle způsobu využití umělé inteligence a oblasti působnosti dané organizace na ni dopadají i další právní povinnosti. Povinnosti podle předpisů, které již jsou, na rozdíl od Aktu o umělé inteligenci, plně účinné a vymahatelné.

Koho se týká Akt o umělé inteligenci?

Začít bychom ale určitě měli obecnou, a celosvětově první, regulací využití umělé inteligence – Aktem o umělé inteligenci. Toto přímo aplikovatelné nařízení bylo na úrovni Evropské unie přijato 13. června 2024. V souvislosti s vývojem, distribucí a využití umělé inteligence ukládá práva a povinnosti různým subjektům, konkrétně:

- Poskytovatelům, tzn. těm, kdo vyvíjí, nechá vyvíjet nebo na trh pod svým jménem uvádí systém umělé inteligence
- Dovozcům, kteří na EU trhu distribuují systém umělé inteligence označený jménem, názvem nebo ochrannou známkou osoby usazené ve třetí zemi
- Zavádějícím subjektům, tzn. organizacím, které systém umělé inteligence implementují a využívají
- Dotčeným fyzickým osobám, tedy lidem, do jejichž práv a svobod může být využitím systému umělé inteligence zasaženo.

Akt o umělé inteligenci nabývá účinnosti postupně

Akt o umělé inteligenci byl vyhlášen 13. června 2024. Jeho jednotlivá ustanovení však nabývají účinnosti takto:

- Od **2. února 2025** jsou již účinná obecná ustanovení Aktu o umělé inteligenci, tzn. působnost nařízení, vymezení povinných subjektů, definice pojmů, povinnost subjektů využívajících AI zajistit edukaci uživatelů a zákaz využití AI pro vysoce rizikové činnosti (např. sociální scoring, zneužívání zranitelností určitých skupin osob, analýza emocí na pracovišti či ve škole atd.).

- Od **2. srpna 2025** začnou být účinná ustanovení o rolích a kompetencích dozorových úřadů v oblasti AI, pravidla pro dozor na EU úrovni a některé povinnosti související s obecnými modely umělé inteligence.
- Od **2. srpna 2026** budou aplikovatelné povinnosti pro organizace vyvíjecí nebo využívající (zavádějící) vysoce rizikové systémy umělé inteligence; těmi se rozumí například systémy pro biometrickou identifikaci na dálku, systémy umělé inteligence využívané v pracovněprávní oblasti či v oblasti vzdělávání, systémy využívané pro vyhodnocení přístupu k některým produktům, jako je spotřebitelský úvěr či životní pojištění atd. Ke stejnému datu budou začnou být rovněž aplikovatelné další povinnosti v oblasti transparentnosti při využití umělé inteligence.
- Od **2. srpna 2027** pak budou účinné zbývající povinnosti, zejména pravidla pro vysoce rizikové systémy umělé inteligence využívaných jako bezpečnostní komponenty v produktové regulaci, například bezpečnost průmyslových výrobků, hraček, vozidel atd., a pravidla pro méně rizikové využití umělé inteligence.

Využití **vysoce rizikových systémů** umělé inteligence bude od příštího roku podléhat řadě detailních povinností. Půjde zejména o povinnost nastavit celkovou správu a kontrolu nad využitím umělé inteligence (AI governance), definovat a zavést proces pro řízení rizik, získat a udržovat aktuální dokumentaci o systému, zajistit lidskou kontrolu, dokumentovat (logovat) fungování systému, informovat o jeho využití dotčené fyzické osoby, např. zaměstnance atd.

Poskytovatelům a dovozcům vysoce rizikových systémů pak příslušná ustanovení Aktu o umělé inteligenci ukládají řadu dalších povinností, od zavedení systému řízení kvality, pořizování dokumentace a povinnou certifikaci nebo prohlášení o shodě, až po registraci v celounijní evidence vysoce rizikových systémů umělé inteligence či automatické generování protokolů o fungování systému, který budou jako službu provozovat.

Rozsah povinností plynoucích z Aktu o umělé inteligenci pro organizace, které využívají nebo budou využívat umělou inteligenci, a rozsah a míra detailu povinností pro poskytovatele či dovozce těchto systémů ze zemí mimo EU, je skutečně velký. Tato skutečnost odůvodňuje obavy o to, zda té regulace není přeci jenom příliš a z Evropské unie si díky ní nevytvoříme technický skanzen.

Až čas ukáže, jaký bude mít Akt o umělé inteligenci dopad na praxi vývoje a využití umělé inteligence v Evropské unii. Již nyní však víme, že využití umělé inteligence podléhá dalším právním předpisům a regulacím, z nichž některé jsou již plně účinné, aplikovatelné a hlavně vymahatelné.

AI a zpracování osobních údajů

Využití systémů umělé inteligence s sebou často nese i zpracování osobních údajů tak, jak je definováno v obecném nařízení o ochraně osobních údajů (GDPR)[3]. Platí jak pro cílené využití umělé inteligence v případě, kdy organizace cíleně využije umělou inteligenci pro automatizaci proces zahrnující zpracování dat, jako je typicky marketingová komunikace, datová analytika, hodnocení zaměstnanců, zákaznická podpora atd. O zpracování osobních údajů se ale bude jednat i v případech, kdy je umělá inteligence využívána v jiných procesech, které primárně s osobními údaji nepracují, protože i zde dochází většinou alespoň k logování aktivit uživatelů, zaměstnanců, a k dalším operacím s těmito osobními daty.

Využití umělé inteligence bude obvykle představovat pouze další (nový) způsob zpracování osobních údajů, nikoliv nové zpracování za samostatným účelem. Organizace by proto měla primárně posoudit, jaká rizika pro dotčené osoby, subjekty údajů, tento systém přináší. Zejména v případě systému provozovaném dodavatelem (AI as a Service) je nutné vyhodnotit, k jakým datům bude mít

provozovatel přístup, kde je bude uchovávat (EU vs. třetí země[4]) a zda je hodlá či může využívat i k dalším účelům a stát se tak správce, samostatným či společným s danou organizací.

U externě i interně využívaných modelů umělé inteligence je nutné především zajistit bezpečnost, integritu a přesnost zpracovávaných osobních údajů a o tomto způsobu zpracování informovat dotčené subjekty údajů. V případě, kdy bude systém využit v rámci automatizovaného zpracování údajů, které má pro dotčenou osobu přímé právní důsledky, musí daná organizace rovněž zajistit splnění specifických podmínek podle čl. 22, jimiž jsou:

- Nutnost aplikovat pouze omezený okruh právních důvodů k takovémuto zpracování osobních údajů; může se jednat o zpracování nezbytné k uzavření či plnění smlouvy, povoleno právem členského státu nebo EU nebo zpracování založeném na výslovném souhlase dotčené osoby.
- Povinnost zavést dodatečná opatření, aby měl dotčený subjekt údajů možnost uplatnit právo na lidský zásah ze strany správce, právo vyjádřit svůj názor a právo napadnout rozhodnutí, které bylo přijato na základě automatizovaného zpracování (s využitím umělé inteligence).
- Až na výjimky tímto systémem nezpracovávat citlivé osobní údaje, např. biometrická data za účelem identifikace, údaje o národnostním či etnickém původu, o náboženském či politickém přesvědčení, sexuální orientaci atd.

Kybernetická bezpečnost

Další právní oblastí, která s využitím umělé inteligence bezprostředně souvisí, je oblast kybernetické bezpečnosti.

Dne 17. ledna tohoto roku nabylo účinnosti nařízení DORA[5], které se týká kybernetické bezpečnosti a provozní odolnosti ve finančním sektoru. Dopadá především na poskytovatele finančních služeb, konkrétně banky, pojišťovny, obchodníky s cennými papíry, platební instituce, některé zprostředkovatele finančních produktů, regulované obchodníky s kryptoaktivy atd., a také na dodavatele, kteří těmto finančním subjektům poskytují informační či komunikační služby[6].

Druhou regulací, který v následujících měsících zasáhne na tisíce či nízké desítky tisíc českých organizací, bude směrnice NIS2[7], resp. tuto směrnici transponující nový zákon o kybernetické bezpečnosti[8]. Ten uloží řadu povinností v oblasti kybernetické bezpečnosti organizacím ze sektorů jako je energetika, doprava, zdravotnictví, ale i nakládání s odpady, poskytování digitálních služeb, výroba a distribuce potravin či veřejné správy a územní samosprávy.

Co mají tyto právní předpisy společného ve vztahu k předmětu našeho článku, využití umělé inteligence?

Oba předpisy regulovaným subjektům ukládají povinnost definovat, evidovat a kontrolovat své kritické procesy a související aktiva a chránit je proti kybernetickým hrozbám. Pokud tato aktiva jsou sama o sobě systémy umělé inteligence, nebo je nástroje využívající umělé inteligence podporují, pak povinné subjekty musí do celkového režimu a pravidel podle nařízení DORA či nového zákona o kybernetické bezpečnosti zahrnout právě i tento informační systém. A i ve vztahu k němu plnit veškeré další povinnosti v oblasti ochrany informací, řízení přístupů, zálohování, monitoringu, zajištění dostupnosti poskytovaných služeb (business continuity) atd.

Jinak řečeno, pokud systém využívající umělou inteligenci podporuje kritické či významné funkce, musí jej organizace chránit tak, jak jí to uvedené předpisy z oblasti kybernetické bezpečnosti ukládají. Což s sebou samozřejmě nese jistá specifika, zejména kvůli charakteru a způsobu fungování umělé inteligence.

Ochrana spotřebitele v éře umělé inteligence

Pokud je umělé inteligence využita pro komunikaci s klienty, fyzickými osobami vystupujícími mimo svoji podnikatelskou činnosti, je nutné zohlednit i pravidla pro ochranu spotřebitele. Týká se to systémů, které buď vyřizují, evidují nebo připravují podklady pro vyřízení podnětů od spotřebitelů, např. žádosti o informace, detaily k produkty, reklamace, stížnosti, dotazy klientů atd. Ve všech těchto situacích může z různých důvodů (nedostatek znalosti či neúplnost tréninkových dat využívaného nástroje, možné algoritmické zkreslení, tzv. AI bias) dojít k tomu, že se spotřebiteli bude jednáno agresivně, klamavě, nepravdivě či diskriminačně. A organizace, která by takto jednala, by mohla porušit zejména zákon č. 634/1992 Sb., o ochraně spotřebitele.

Jak riziku poškození práv spotřebitele při využití umělé inteligence předejít?

U systémů umělé inteligence, které takto přímo či nepřímo zajišťují komunikaci se spotřebiteli, je vhodné přijmout přiměřená opatření ke kontrole, monitoringu a možnosti rychlé úpravy jejich výstupů. V případě externě využívaných systémů (AI as a Service) se bude jednat především o získání dokumentace od poskytovatele, včetně ověření dat využitých k tréninku modelu. Pro externě i interně provozovaný systém je pak vhodné je nejprve otestovat na omezeném vzorku případů a v nich vyhodnotit, zda výstupy nejsou v rozporu se spotřebitelskou regulací, zajistit průběžný monitoring a lidskou kontrolu nad systémem a transparentní informování dotčených osob o tom, že s nimi přímo či nepřímo bude interreagovat systém umělé inteligence.

Sektorová regulace upravuje specifické podmínky využití AI

Právní předpisy v řadě sektorů ukládají další povinnosti, které je pochopitelně nutné plnit i tehdy, pokud jsou při poskytování regulovaných služeb zahrnuty i prvky či systémy umělé inteligence. Typicky se jedná o nabízení či zprostředkování finančních produktů, při kterým finanční instituce musí například zajistit uchování záznamů o komunikaci s klienty[9], jsou povinny zajistit rekonstruovatelnost komunikace a vzájemné interakce s klientem[10] a poskytovat zájemci o produkt širokou řadu informací[11].

Všechny tyto povinnosti platí i při využití systémů umělé inteligence, ať už se jedná o distribuci spotřebitelského úvěru či životního pojištění, které Akt o umělé inteligenci řadí mezi tzv. vysoce rizikové systémy, nebo jakýkoliv další produkt (jiný druh pojištění, investice, služby elektronických komunikací[12], atd.).

Právních rizik spojených s AI je ještě více!

Využití systémů umělé inteligence s sebou již dnes, před plnou účinností Aktu o umělé inteligenci, nese řadu dalších právních povinností a rizik. Za všechny jmenujme například otázky spojené s autorským právem, ať už ve vztahu k riziku souvisejícímu s daty, na kterých je model trénován, nebo k riziku týkajícího se autorských práv, resp. práva na využití výstupu ze systému umělé inteligence.

I když Akt o umělé inteligenci bude v plném rozsahu aplikovatelný až v roce 2027, využití umělé inteligence musí být již dnes v souladu s dalšími právním předpisy. Jinak se organizace, které takové systémy vyvíjejí či zavádějí, vystavují riziku právního postihu, včetně pokut.

Mgr. František Nonnemann,

autor je vedoucím oddělení Compliance a oddělení Řízení operačního rizika ve společnosti Partners Banka, a.s.

Článek odráží skutkový a právní stav k 2. červnu 2025 a vyjadřuje osobní názor autora.

e-mail: nonnemann@volny.cz

---

[1] Pro účely tohoto článku je pojem umělá inteligence využíván dle definice v čl. 3 bodu 1) Aktu o umělé inteligenci: „Systémem AI [se rozumí] strojový systém navržený tak, aby po zavedení fungoval s různými úrovněmi autonomie a který po zavedení může vykazovat adaptabilitu a který za explicitními nebo implicitními účely z obdržených vstupů odvozuje, jak generovat výstupy, jako jsou predikce, obsah, doporučení nebo rozhodnutí, které mohou ovlivnit fyzická nebo virtuální prostředí."

[2] Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

[3] Nařízení Evropského parlamentu a Rady (EU) ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

[4] Viz pravidla pro předávání osobních údajů mimo EU/EHS upravená v čl. 44 a dále GDPR.

[5] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011.

[6] Tento pojem je přitom v čl. 3 bod 21 nařízení DORA vymezen poměrně široce takto: „Službami IKT [se rozumí] digitální a datové služby poskytované prostřednictvím systémů IKT průběžně jednomu nebo více interním nebo externím uživatelům, včetně hardwaru jako služby a hardwarových služeb, které zahrnují poskytování technické podpory prostřednictvím aktualizací softwaru nebo firmwaru poskytovatelem hardwaru, s výjimkou tradičních analogových telefonních služeb."

[7] Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2).

[8] V době odevzdání tohoto článku je návrh nového zákona o kybernetické bezpečnosti projednáván Senátem. Účinnost nového zákona lze očekávat na konci roku 2025 či na samém počátku roku 2026.

[9] Viz například § 79–80 zákona č. 170/2018 Sb., o distribuci pojištění a zajištění, nebo § 15 a násl. zákona č. 256/2004 Sb., o podnikání na kapitálovém trhu.

[10] Např. dle § 78 zákona č. 257/2016 Sb., o spotřebitelském úvěru.

[11] Pro ilustraci srov. § 132 a dále zákona č. 370/2017 Sb., o platebním styku.

[12] Viz zákon č. 127/2005 Sb., o elektronických komunikacích.

Další články:

- 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?
- Zápis ochranné známky bez komplikací. Klíčem k úspěchu je kvalitní předběžná rešerše
- Zneužití práva na přístup podle GDPR
- Byznys a paragrafy, díl 31. - létající pořizovatel ve světle nového stavebního zákona
- Právní povaha sítě elektronických komunikací – režim náhrady škody
- Náhrada ušlého nájemného při předčasném ukončení nájemní smlouvy na nebytové prostory
- Jak fungují plánovací smlouvy v reálných situacích (2. díl)