Umělá inteligence – otázky a odpovědi

Proč potřebujeme regulovat používání umělé inteligence?

A. Zákon EU o umělé inteligenci je prvním komplexním zákonem o umělé inteligenci na světě. Jeho cílem je řešit rizika pro zdraví, bezpečnost a základní práva. Nařízení také chrání demokracii, právní stát a životní prostředí.

B. Zavádění systémů umělé inteligence má velký potenciál přinést společenské výhody, hospodářský růst a posílit inovace EU a globální konkurenceschopnost. V určitých případech však mohou specifické vlastnosti určitých systémů umělé inteligence vytvářet nová rizika související s bezpečností uživatelů, včetně fyzické bezpečnosti, a základních práv. Některé výkonné modely umělé inteligence, které jsou široce používány, mohou dokonce představovat systémová rizika.

C. To vede k právní nejistotě a potenciálně pomalejšímu zavádění technologií umělé inteligence veřejnými orgány, podniky a občany kvůli nedostatku důvěry. Nesourodé regulační reakce vnitrostátních orgánů by hrozily roztříštěním vnitřního trhu.

D. V reakci na tyto výzvy bylo zapotřebí legislativních opatření k zajištění dobře fungujícího vnitřního trhu pro systémy umělé inteligence, kde jsou náležitě řešeny přínosy i rizika.

Na koho se vztahuje zákon o AI?

Právní rámec se bude vztahovat na veřejné i soukromé subjekty v EU i mimo ni, pokud bude systém umělé inteligence uváděn na trh Unie nebo pokud bude mít jeho používání dopad na osoby nacházející se v EU.

Povinnosti se mohou dotknout jak poskytovatelů (např. vývojáře nástroje pro prověřování životopisů), tak uživatelů systémů umělé inteligence (např. banky, která tento nástroj pro prověřování nakupuje). Z nařízení existují určité výjimky. Činnosti výzkumu, vývoje a prototypování, které probíhají před uvedením systému umělé inteligence na trh, těmto předpisům nepodléhají. Kromě toho jsou osvobozeny také systémy umělé inteligence, které jsou výhradně navrženy pro vojenské, obranné nebo národní bezpečnostní účely, bez ohledu na typ subjektu provádějícího tyto činnosti.

Jaké jsou rizikové kategorie?

Zákon o AI zavádí jednotný rámec pro všechny členské státy EU, založený na progresivní definici AI a přístupu založeném na riziku:

Nepřijatelné riziko : Velmi omezený soubor zvláště škodlivých způsobů použití umělé inteligence, které jsou v rozporu s hodnotami EU, protože porušují základní práva, a proto budou zakázány:

- Využívání zranitelnosti osob, manipulace a používání podprahových technik;
- Sociální hodnocení pro veřejné a soukromé účely;
- Individuální prediktivní policejní práce založená výhradně na profilování osob;
- Necílené seškrabování z internetu nebo CCTV pro snímky obličejů za účelem vytváření nebo rozšiřování databází;
- rozpoznávání emocí na pracovišti a ve vzdělávacích institucích , s výjimkou lékařských nebo bezpečnostních důvodů (tj. sledování úrovně únavy pilota);

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

- Biometrická kategorizace fyzických osob za účelem odvození nebo vyvození jejich rasy, politických názorů, členství v odborech, náboženského nebo filozofického přesvědčení nebo sexuální orientace. Označování nebo filtrování datových sad a kategorizace dat v oblasti vymáhání práva bude i nadále možné;
- Vzdálená biometrická identifikace v reálném čase ve veřejně přístupných prostorách ze strany orgánů činných v trestním řízení, až na úzké výjimky (viz níže).

Komise vydá pokyny k zákazům před jejich vstupem v platnost dne 2. února 2025.

Vysoce rizikové : Omezený počet systémů umělé inteligence definovaných v návrhu, které mohou mít nepříznivý dopad na bezpečnost lidí nebo jejich základní práva (jak jsou chráněna Listinou základních práv EU), je považován za vysoce rizikový. V příloze zákona jsou uvedeny seznamy vysoce rizikových systémů umělé inteligence, které lze revidovat, aby odpovídaly vývoji případů použití umělé inteligence.

- Patří sem také bezpečnostní součásti výrobků, na které se vztahují odvětvové právní předpisy Unie. Budou vždy považovány za vysoce rizikové, pokud budou předmětem posouzení shody třetí stranou podle těchto odvětvových právních předpisů.
- Mezi tyto vysoce rizikové systémy umělé inteligence patří například systémy umělé inteligence, které posuzují, zda je někdo schopen podstoupit určité lékařské ošetření, získat určitou práci nebo půjčku na koupi bytu. Dalšími vysoce rizikovými systémy umělé inteligence jsou systémy, které policie používá k profilování osob nebo k posouzení jejich rizika spáchání trestného činu (pokud to nezakazuje článek 5). A vysoce rizikové mohou být také systémy umělé inteligence provozující roboty, drony nebo lékařská zařízení.

Specifické riziko transparentnosti : Pro posílení důvěry je důležité zajistit transparentnost ohledně používání AI. Zákon o AI proto zavádí specifické požadavky na transparentnost pro určité aplikace AI, například tam, kde existuje jasné riziko manipulace (např. pomocí chatbotů) nebo deep fake. Uživatelé by si měli být vědomi toho, že interagují se strojem.

Minimální riziko : Většinu systémů umělé inteligence lze vyvíjet a používat v souladu se stávající legislativou bez dalších právních povinností. Poskytovatelé těchto systémů se mohou dobrovolně rozhodnout uplatňovat požadavky na důvěryhodnou umělou inteligenci a dodržovat dobrovolné kodexy chování.
Zákon o AI navíc zohledňuje systémová rizika , která by mohla vyplynout rizika, modelů AI, včetně velkých generativních modelů AI . Ty lze použít pro různé úkoly a stávají se základem mnoha systémů umělé inteligence v EU. Některé z těchto modelů by mohly nést systémová rizika, pokud jsou velmi schopné nebo široce používané. Výkonné modely by například mohly způsobit vážné nehody nebo být zneužity k dalekosáhlým kybernetickým útokům. Mnoho jednotlivců může být ovlivněno, pokud model šíří škodlivé zkreslení v mnoha aplikacích.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Jak zjistím, zda je systém umělé inteligence vysoce rizikový?

Zákon o umělé inteligenci stanoví pevnou metodiku pro klasifikaci systémů umělé inteligence jako vysoce rizikové. Cílem je poskytnout právní jistotu pro podniky a další provozovatele.

Klasifikace rizik je založena na zamýšleném účelu systému umělé inteligence v souladu se stávajícími právními předpisy EU o bezpečnosti výrobků. To znamená, že klasifikace závisí na funkci vykonávané systémem AI a na konkrétním účelu a modalitách, pro které je systém používán.

Systémy AI lze klasifikovat jako vysoce rizikové ve dvou případech:

- Pokud je systém umělé inteligence zabudován jako bezpečnostní součást do výrobků, na které se vztahují stávající právní předpisy o výrobcích (příloha I), nebo takové výrobky samy tvoří. Může to být například lékařský software založený na umělé inteligenci.
- Pokud je systém umělé inteligence určen k použití pro vysoce rizikový případ použití uvedený v příloze III zákona o umělé inteligenci. Seznam zahrnuje případy použití z oblastí, jako je vzdělávání, zaměstnání, vymáhání práva nebo migrace.

Komise připravuje pokyny pro klasifikaci vysokého rizika, které budou zveřejněny před datem použití těchto pravidel.

Jaké jsou příklady vysoce rizikových případů použití definovaných v příloze III?

Příloha III obsahuje osm oblastí, ve kterých může být použití umělé inteligence obzvláště citlivé, a uvádí konkrétní případy použití pro každou oblast. Systém umělé inteligence je klasifikován jako vysoce rizikový, pokud je určen k použití pro jeden z těchto případů použití.

Příklady:

- systémy umělé inteligence používané jako bezpečnostní komponenty v určitých kritických infrastrukturách, například v oblasti silniční dopravy a dodávek vody, plynu, topení a elektřiny;
- systémy umělé inteligence používané ve vzdělávání a odborné přípravě, např. k hodnocení výsledků učení a řízení procesu učení a sledování podvádění;
- Systémy umělé inteligence používané při řízení zaměstnanosti a pracovníků a přístupu k samostatné výdělečné činnosti, např. k podávání cílených pracovních nabídek, k analýze a filtrování žádostí o zaměstnání a k hodnocení kandidátů;
- systémy umělé inteligence používané pro přístup k základním soukromým a veřejným službám a výhodám (např. zdravotní péče), hodnocení), hodnocení osob a hodnocení rizik a cen ve vztahu k životnímu a zdravotnímu pojištění ;
- systémy umělé inteligence používané v oblasti vymáhání práva , migrace a kontroly hranic , pokud již nejsou zakázány, a rovněž při práva, a demokratických procesů ;

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

- Systémy umělé inteligence používané pro biometrickou identifikaci, biometrickou kategorizaci a rozpoznávání emocí, pokud nejsou zakázány.

Jaké povinnosti mají poskytovatelé vysoce rizikových systémů umělé inteligence?

Před uvedením vysoce rizikového systému umělé inteligence na trh EU nebo jiným jeho uvedením do provozu jej poskytovatelé musí podrobit posouzení shody . To jim umožní prokázat, že jejich systém splňuje povinné požadavky na důvěryhodnou AI (např. kvalita dat, dokumentace a sledovatelnost, transparentnost, lidský dohled, přesnost, kybernetická bezpečnost a robustnost). Toto posouzení se musí opakovat, pokud se systém nebo jeho účel podstatně změní.

Systémy umělé inteligence, které slouží jako bezpečnostní komponenty produktů, na které se vztahují odvětvové právní předpisy Unie, budou vždy považovány za vysoce rizikové, pokud budou podléhat posouzení shody třetí stranou podle těchto odvětvových právních předpisů. Kromě toho budou všechny biometrické systémy bez ohledu na jejich použití vyžadovat posouzení shody třetí stranou.

Poskytovatelé vysoce rizikových systémů umělé inteligence budou muset zavést systémy řízení kvality a rizik , aby zajistili jejich soulad s novými požadavky a minimalizovali rizika pro uživatele a dotčené osoby, a to i po uvedení produktu na trh.

Vysoce rizikové systémy umělé inteligence, které zavádějí veřejné orgány nebo subjekty jednající jejich jménem, budou muset být zaregistrovány ve veřejné databázi EU , pokud se tyto systémy nepoužívají k vymáhání práva a migraci. Ten bude muset být registrován v neveřejné části databáze, která bude přístupná pouze příslušným dozorovým orgánům.

Aby byla zajištěna shoda v průběhu celého životního cyklu systému umělé inteligence, budou orgány dozoru nad trhem provádět pravidelné audity a usnadňovat monitorování po uvedení na trh a umožní poskytovatelům dobrovolně hlásit jakékoli závažné incidenty nebo porušení povinností v oblasti základních práv, o kterých se dozvědí. Ve výjimečných případech mohou orgány udělit výjimky pro konkrétní vysoce rizikové systémy umělé inteligence, které mají být uvedeny na trh.

V případě porušení požadavky umožní vnitrostátním orgánům mít přístup k informacím potřebným k prošetření, zda použití systému umělé inteligence bylo v souladu se zákonem.

Jaká by byla role standardizace v zákoně o umělé inteligenci?

Podle zákona o umělé inteligenci budou vysoce rizikové systémy umělé inteligence podléhat zvláštním požadavkům. Evropské harmonizované normy budou hrát klíčovou roli při provádění těchto požadavků.

V květnu 2023 Evropská komise pověřila evropské normalizační organizace CEN a CENELEC vypracováním norem pro tyto vysoce rizikové požadavky. Tento mandát bude nyní pozměněn, aby byl v souladu s konečným zněním zákona o umělé inteligenci.

Evropské normalizační organizace budou mít čas do konce dubna 2025 na vývoj a zveřejnění norem. Komise poté vyhodnotí a případně schválí tyto normy, které budou zveřejněny v Úředním věstníku EU. Jakmile budou tyto normy zveřejněny, zaručují „předpoklad shody“ systémům umělé inteligence vyvinutým v souladu s nimi.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Jak jsou regulovány modely umělé inteligence pro obecné účely?

Univerzální modely umělé inteligence, včetně velkých inteligence, včetně umělé inteligence , lze použít pro různé úkoly. Jednotlivé modely lze integrovat do velkého množství systémů AI.
Je zásadní, aby poskytovatel systému umělé inteligence integrující model umělé inteligence měl přístup ke všem nezbytným informacím, aby byl systém bezpečný a v souladu se zákonem o umělé inteligenci.
Proto zákon o AI ukládá poskytovatelům takových modelů povinnost sdělit určité informace poskytovatelům navazujících systémů. Tato transparentnost umožňuje lepší pochopení těchto modelů.
Poskytovatelé modelů navíc potřebují mít zavedeny zásady, které zajistí, že při školení svých modelů budou respektovat autorské právo .
Některé z těchto modelů by navíc mohly představovat systémová rizika , protože jsou velmi schopné nebo široce používané.

V současné době se obecné modely umělé inteligence, které byly trénovány s použitím celkového výpočetního výkonu více než 10^25 FLOP, považují za systémové riziko. Komise může tuto prahovou hodnotu aktualizovat nebo doplnit s ohledem na technologický pokrok a může také označit jiné modely za modely představující systémová rizika na základě dalších kritérií (např. počet uživatelů nebo stupeň autonomie modelu).
Poskytovatelé modelů se systémovými riziky jsou povinni vyhodnocovat a zmírňovat rizika , hlásit závažné incidenty , provádět nejmodernější testy a hodnocení modelů a rizika, rizika, modelů.
Poskytovatelé se vyzývají, aby spolupracovali s AI Office a dalšími zúčastněnými stranami na vývoji Kodexu postupů, který podrobně popisuje pravidla, a tím zajišťuje bezpečný a odpovědný vývoj jejich modelů. Tento kodex by měl představovat centrální nástroj pro poskytovatele univerzálních modelů umělé inteligence k prokázání souladu.

Proč je 10^25 FLOP vhodnou hranicí pro GPAI se systémovými riziky?

FLOP je zástupcem schopností modelu a přesný práh FLOP může Komise aktualizovat směrem nahoru nebo dolů, např. s ohledem na pokrok v objektivním měření schopností modelu a na vývoj výpočetního výkonu potřebného pro danou úroveň výkonu.
Schopnosti modelů nad tímto prahem ještě nejsou dostatečně pochopeny. Mohly by představovat systémová rizika, a proto je rozumné podřídit jejich poskytovatelům další soubor povinností.

Jaké jsou povinnosti týkající se vodoznaku a označování výstupů AI stanovené zákonem o AI?

Zákon o umělé inteligenci stanoví pravidla transparentnosti pro obsah vytvářený generativní umělou inteligencí, aby se vyřešilo riziko manipulace, klamání a dezinformací.

Poskytovatelům generativních systémů umělé inteligence ukládá povinnost označit výstupy umělé inteligence ve strojově čitelném formátu a zajistit, aby byly zjistitelné jako uměle vytvořené nebo zmanipulované. Technická řešení musí být účinná, interoperabilní, robustní a spolehlivá, pokud je to technicky proveditelné, s přihlédnutím ke specifikům a omezením různých typů obsahu, nákladům na implementaci a obecně uznávanému stavu techniky, jak se může odrazit v příslušných technických normách.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Kromě toho musí uživatelé generativních systémů umělé inteligence, kteří generují nebo manipulují s obrazovým, zvukovým nebo obrazovým obsahem představujícím hluboké padělky, viditelně odhalit, že obsah byl uměle vytvořen nebo zmanipulován. Nasazení systému umělé inteligence, který generuje nebo manipuluje s textem publikovaným za účelem informování veřejnosti o záležitostech veřejného zájmu, musí také prozradit, že text byl uměle vytvořen nebo zmanipulován. Tato povinnost se nevztahuje na případy, kdy obsah generovaný umělou inteligencí prošel procesem lidské kontroly nebo redakční kontroly a kdy za zveřejnění obsahu nese redakční odpovědnost fyzická nebo právnická osoba.

Úřad pro umělou inteligenci vydá pokyny k poskytování dalších pokynů pro poskytovatele a poskytovatele služeb ohledně povinností podle článku 50, které se stanou použitelnými dva roky po vstupu zákona o umělé inteligenci v platnost (2. srpna 2026).

Kancelář pro umělou inteligenci bude rovněž podporovat a usnadňovat vypracování kodexů správné praxe na úrovni Unie s cílem zefektivnit účinné provádění povinností souvisejících s odhalováním a označováním uměle vytvořeného nebo zmanipulovaného obsahu.

Je zákon o umělé inteligenci odolný vůči budoucnosti?

Zákon o AI nastavuje právní rámec, který reaguje na nový vývoj, snadno a rychle se přizpůsobuje a umožňuje časté hodnocení.
Zákon o AI stanovuje požadavky a povinnosti orientované na výsledky, ale konkrétní technická řešení a provozování ponechává na standardech a kodexech praxe řízených průmyslem, které jsou flexibilní, aby se přizpůsobily různým případům použití a umožnily nová technologická řešení.
Kromě toho mohou být právní předpisy samotné pozměněny akty v přenesené pravomoci a prováděcími akty, například za účelem přezkumu seznamu vysoce rizikových případů použití v příloze III.
A konečně dojde k častým hodnocením některých částí zákona o AI a případně i celého nařízení, aby bylo zajištěno, že bude identifikována jakákoli potřeba revize a novelizace.

Jak zákon o AI upravuje biometrickou identifikaci?

Používání biometrické identifikace na dálku v reálném čase ve veřejně přístupných prostorách (tj. rozpoznávání obličeje pomocí CCTV) pro účely vymáhání práva je zakázáno. Členské státy mohou zákonem zavést výjimky, které by umožnily použití biometrické identifikace na dálku v reálném čase v těchto případech:

Činnost činná v trestním řízení se týkala 16 specifikovaných velmi závažných trestných činů;

- cílené vyhledávání konkrétních obětí, únosů, obchodování s lidmi a sexuálního vykořisťování lidí a pohřešovaných osob; nebo
- Prevence ohrožení života nebo fyzické bezpečnosti osob nebo reakce na současnou nebo předvídatelnou hrozbu teroristického útoku.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Jakékoli výjimečné použití by podléhalo předchozímu povolení soudního nebo nezávislého správního orgánu, jehož rozhodnutí je závazné. V naléhavých případech lze souhlas udělit do 24 hodin; pokud je autorizace zamítnuta, všechna data a výstup musí být smazány.

Muselo by mu předcházet předchozí posouzení dopadu na základní práva a mělo by být oznámeno příslušnému orgánu dozoru nad trhem a orgánu pro ochranu údajů . V naléhavých případech může být používání systému zahájeno bez registrace.

Použití systémů umělé inteligence k následné biometrické identifikaci na dálku (identifikace osob v dříve shromážděných materiálech) vyšetřovaných osob vyžaduje předchozí povolení soudního orgánu nebo nezávislého správního orgánu a také oznámení příslušnému orgánu pro ochranu údajů a dozor nad trhem.

Proč jsou pro vzdálenou biometrickou identifikaci potřebná zvláštní pravidla?
Biometrická identifikace může mít různé podoby. Biometrická autentizace a verifikace, tj. odemknutí chytrého telefonu nebo ověření/ověření na hraničních přechodech za účelem ověření totožnosti osoby s jejími cestovními doklady (jednotné shody), zůstávají neregulované, protože nepředstavují významné riziko pro základní práva.

Naproti tomu biometrickou identifikaci lze použít i na dálku, například k identifikaci osob v davu, což může výrazně ovlivnit soukromí ve veřejném prostoru.

Přesnost systémů pro rozpoznávání obličeje může být významně ovlivněna širokou škálou faktorů, jako je kvalita fotoaparátu, světlo, vzdálenost, databáze, algoritmus a etnický původ, věk nebo pohlaví subjektu. Totéž platí pro rozpoznávání chůze a hlasu a další biometrické systémy. Vysoce pokročilé systémy neustále snižují míru falešného přijetí.

I když se 99% přesnost může zdát obecně dobrá, je značně riskantní, když výsledek může vést k podezření na nevinnou osobu. Dokonce i 0,1% chybovost může mít významný dopad, pokud je aplikována na velké populace, například na vlakových nádražích.

Jak pravidla chrání základní práva?

Na úrovni EU a členských států již existuje silná ochrana základních práv a nediskriminace, ale složitost a neprůhlednost některých aplikací umělé inteligence („černé skříňky“) může představovat problém.

Přístup k umělé inteligenci zaměřený na člověka znamená zajistit, aby aplikace umělé inteligence byly v souladu s právními předpisy o základních právech. Začleněním požadavků na odpovědnost a transparentnost do vývoje vysoce rizikových systémů umělé inteligence a zlepšením možností prosazování můžeme zajistit, že tyto systémy jsou od začátku navrženy s ohledem na soulad s právními předpisy. Pokud dojde k porušení, takové požadavky umožní

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

vnitrostátním orgánům mít přístup k informacím potřebným k prošetření, zda použití umělé inteligence bylo v souladu s právem EU.

Zákon o umělé inteligenci navíc vyžaduje, aby někteří uživatelé vysoce rizikových systémů umělé inteligence provedli posouzení dopadu na základní práva.

Co je posouzení dopadu na základní práva? Kdo a kdy musí takové posouzení provést?

Poskytovatelé vysoce rizikových systémů umělé inteligence musí provést posouzení rizik a navrhnout systém tak, aby rizika pro zdraví, bezpečnost a základní práva byla minimalizována.

Některá rizika pro základní práva však lze plně identifikovat pouze se znalostí kontextu používání vysoce rizikového systému umělé inteligence. Jsou-li vysoce rizikové systémy umělé inteligence používány ve zvláště citlivých oblastech s možnou asymetrií výkonu, jsou nezbytná další zvážení takových rizik.

Zavádějící subjekty, které jsou veřejnoprávními subjekty nebo soukromí provozovatelé poskytující veřejné služby, jakož i provozovatelé poskytující vysoce rizikové systémy umělé inteligence, kteří provádějí hodnocení úvěruschopnosti nebo hodnocení cen a rizik v životním a zdravotním pojištění, proto provedou posouzení dopadu na základní práva a oznámí výsledky vnitrostátnímu orgánu.

V praxi bude muset mnoho poskytovatelů také provést posouzení dopadu na ochranu údajů. Aby se v takových případech zabránilo podstatnému překrývání, posouzení dopadu na základní práva se provede společně s tímto posouzením dopadu na ochranu údajů.

Jak toto nařízení řeší rasové a genderové předsudky v AI?

Je velmi důležité zdůraznit, že systémy umělé inteligence nevytvářejí ani nereprodukují zkreslení . Pokud jsou systémy umělé inteligence správně navrženy a používány, mohou spíše přispívat ke snižování zaujatosti a stávající strukturální diskriminace , a vést tak ke spravedlivějším a nediskriminačním rozhodnutím (např. při náboru).

Tomuto účelu poslouží nové povinné požadavky na všechny vysoce rizikové systémy umělé inteligence . Systémy umělé inteligence musí být technicky odolné , aby bylo zajištěno, že budou vhodné pro daný účel a nebudou produkovat zkreslené výsledky, jako jsou falešně pozitivní nebo negativní výsledky, které neúměrně ovlivňují marginalizované skupiny, včetně těch, které jsou založeny na rasovém nebo etnickém původu, pohlaví, věku a dalších chráněných charakteristikách.

Systémy s vysokým rizikem budou také muset být vyškoleny a testovány s dostatečně reprezentativními soubory dat, aby se minimalizovalo riziko nespravedlivých dat, aby do modelu a zajistilo se, že je lze řešit pomocí vhodného odhalování, nápravy a dalších zmírňujících opatření.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Musí být také sledovatelné a kontrolovatelné , což zajistí, kontrolovatelné, uchovávána příslušná dokumentace , včetně údajů používaných k trénování algoritmu, který by byl klíčový při vyšetřování ex post.

Compliance System před a po jejich uvedení na trh bude muset zajistit, aby tyto systémy byly pravidelně monitorovány a případná rizika byla rychle řešena .

Kdy bude zákon o umělé inteligenci plně aplikovatelný?

Zákon o umělé inteligenci se použije dva roky po vstupu v platnost dne **2. srpna 2026**, s výjimkou následujících zvláštních ustanovení:

- Zákazy, definice a ustanovení týkající se gramotnosti umělé inteligence budou platit 6 měsíců po vstupu v platnost dne 2. února 2025;
- Pravidla pro správu a řízení a povinnosti pro AI pro obecné účely se stanou použitelnými 12 měsíců po vstupu v platnost dne 2. srpna 2025;
- Povinnosti pro vysoce rizikové systémy umělé inteligence, které jsou klasifikovány jako vysoce rizikové, protože jsou součástí regulovaných produktů, uvedené v příloze II (seznam harmonizačních právních předpisů Unie), platí 36 měsíců po vstupu v platnost dne 2. srpna 2027.

Jak bude prosazován zákon o AI?

Zákon o umělé inteligenci zavádí dvouúrovňový systém řízení, kde jsou vnitrostátní orgány odpovědné za dohled a vymáhání pravidel pro systémy umělé inteligence, zatímco úroveň EU odpovídá za řízení modelů umělé inteligence pro obecné účely.

K zajištění soudržnosti a spolupráce v rámci celé EU bude zřízena Evropská rada pro umělou inteligenci (AI Board), složená ze zástupců členských států, se specializovanými podskupinami pro vnitrostátní regulační orgány a další příslušné orgány.

Úřad pro umělou inteligenci , prováděcí orgán Komise pro zákon o umělé inteligenci, bude poskytovat Radě pro umělou inteligenci strategické vedení.

Kromě toho zákon o umělé inteligenci zřizuje dva poradní orgány, které poskytují odborné příspěvky: Vědecký panel a Poradní fórum . Tyto orgány nabídnou cenné poznatky od zúčastněných stran a interdisciplinárních vědeckých komunit, budou poskytovat informace pro rozhodování a zajistí vyvážený přístup k rozvoji umělé inteligence.

Proč je potřeba Evropská rada pro umělou inteligenci a co bude dělat?

Evropský výbor pro umělou inteligenci se skládá ze zástupců členských států na vysoké úrovni a evropského inspektora ochrany údajů. Rada pro umělou inteligenci jako klíčový poradce poskytuje poradenství ve všech záležitostech

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

souvisejících s politikou umělé inteligence, zejména s regulací umělé inteligence, politikou inovací a excelence a mezinárodní spoluprací v oblasti umělé inteligence.

Rada AI hraje klíčovou roli při zajišťování hladkého, efektivního a harmonizovaného provádění zákona o AI. Rada bude sloužit jako fórum, kde mohou regulátoři umělé inteligence, jmenovitě Úřad pro umělou inteligenci, vnitrostátní orgány a EPDS, koordinovat důsledné uplatňování zákona o umělé inteligenci.

Jaké jsou sankce za porušení?

Členské státy budou muset stanovit účinné, přiměřené a odrazující sankce za porušení pravidel pro systémy umělé inteligence.

Nařízení stanoví prahové hodnoty, které je třeba vzít v úvahu:

- až 35 milionů EUR nebo 7 % z celkového celosvětového ročního obratu za předchozí finanční rok (podle toho, co je vyšší) za porušení zakázaných postupů nebo nedodržení požadavků na údaje;
- Až 15 milionů EUR nebo 3 % z celkového celosvětového ročního obratu za předchozí finanční rok za nedodržení jakýchkoli jiných požadavků nebo povinností Nařízení;
- až 7,5 milionu EUR nebo 1,5 % z celkového celosvětového ročního obratu za předchozí finanční rok za poskytnutí nesprávných, neúplných nebo zavádějících informací oznámeným subjektům a příslušným vnitrostátním orgánům v odpovědi na žádost;

Pro každou kategorii porušení by prahová hodnota byla nižší ze dvou částek pro malé a střední podniky a vyšší pro ostatní společnosti. Komise může rovněž vymáhat pravidla pro poskytovatele modelů umělé inteligence pro obecné účely prostřednictvím pokut, přičemž zohlední následující prahovou hodnotu:

Až 15 milionů EUR nebo 3 % z celkového celosvětového ročního obratu v předchozím finančním roce za nedodržení jakékoli z povinností nebo opatření požadovaných Komisí podle nařízení.
Od orgánů, agentur nebo orgánů EU se očekává, že půjdou příkladem, a proto budou také podléhat pravidlům a případným sankcím. Evropský inspektor ochrany údajů bude mít pravomoc ukládat jim pokuty v případě nedodržení.

Jak bude sepsán kodex obecné praxe umělé inteligence?

Vypracování prvního kodexu se řídí komplexním a transparentním procesem. K usnadnění procesu opakovaného navrhování bude zřízeno plénum kodexu postupů, které se bude skládat ze všech zainteresovaných a způsobilých poskytovatelů univerzálních modelů umělé inteligence, navazujících poskytovatelů integrujících univerzální model umělé inteligence do svého systému umělé inteligence, dalších průmyslových organizací, dalších organizací zúčastněných stran, jako je občanská společnost nebo organizace držitelů práv, jakož i z akademické obce a dalších nezávislých odborníků.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Kancelář AI vyhlásila výzvu k vyjádření zájmu o účast na vypracování prvního kodexu. Souběžně s touto výzvou k vyjádření zájmu je zahájena konzultace s mnoha zúčastněnými stranami s cílem shromáždit názory a podněty všech zainteresovaných stran k prvnímu kodexu správné praxe. Odpovědi a příspěvky budou tvořit základ první iterace návrhu Kodexu. Kodex je proto od počátku založen na široké škále úhlů pohledu a odborných znalostí.

Plenární zasedání bude strukturováno do čtyř pracovních skupin, které umožní cílené diskuse o konkrétních tématech souvisejících s podrobným stanovením povinností poskytovatelů univerzálních modelů umělé inteligence a univerzálních modelů umělé inteligence se systémovým rizikem. Účastníci plenárního zasedání si mohou vybrat jednu nebo více pracovních skupin, do kterých se chtějí zapojit. Zasedání probíhají výhradně online.

Kancelář AI jmenuje předsedy a případně místopředsedy pro každou ze čtyř pracovních skupin pléna, vybrané ze zainteresovaných nezávislých odborníků. Předsedové syntetizují příspěvky a připomínky účastníků plenárního zasedání, aby mohli opakovaně navrhnout první kodex postupů.

Jako hlavní adresáti kodexu budou poskytovatelé univerzálních modelů umělé inteligence zváni na specializované workshopy, aby přispěli k informování každého iterativního kola navrhování, kromě své účasti na plenárním zasedání.

Po 9 měsících bude konečná verze prvního kodexu představena na závěrečném plenárním zasedání, které se očekává v dubnu, a zveřejněno. Závěrečné plenární zasedání dává poskytovatelům univerzálních modelů umělé inteligence příležitost vyjádřit se, zda mají v úmyslu Kodex používat.

Jak bude kodex pro poskytovatele univerzálních modelů umělé inteligence v případě schválení sloužit jako centrální nástroj pro dodržování předpisů?

Na konci procesu tvorby kodexu AI Office a AI Board posoudí přiměřenost kodexu a své hodnocení zveřejní. Po tomto posouzení může Komise rozhodnout o schválení kodexu a dát mu obecnou platnost v Unii prostřednictvím prováděcích aktů. Pokud v době, kdy se nařízení stane použitelným, nebude Kodex pro AI považovat za adekvátní, může Komise stanovit společná pravidla pro provádění příslušných povinností.

Poskytovatelé univerzálních modelů umělé inteligence se proto mohou spolehnout na kodex, aby prokázali dodržování povinností stanovených zákonem o umělé inteligenci.

Podle zákona o umělé inteligenci by měl Kodex obsahovat cíle, opatření a případně klíčové ukazatele výkonnosti (KPI).

Poskytovatelé dodržující Kodex by měli Kanceláři pro umělou inteligenci pravidelně podávat zprávy o provádění přijatých opatření a jejich výsledcích, včetně případných měření podle klíčových ukazatelů výkonnosti.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

To usnadňuje vymáhání ze strany Úřadu pro umělou inteligenci, které se opírá o pravomoci dané Komisi zákonem o umělé inteligenci. To zahrnuje schopnost provádět hodnocení modelů umělé inteligence pro obecné účely, vyžadovat informace a opatření od poskytovatelů modelů a uplatňovat sankce.

Úřad pro umělou inteligenci bude podle potřeby podporovat a usnadňovat revizi a přizpůsobení Kodexu tak, aby odrážel pokrok v technologii a nejnovější stav techniky.

Jakmile bude harmonizovaná norma zveřejněna a Úřadem pro umělou inteligenci posouzena jako vhodná pro pokrytí příslušných povinností, měla by shoda s evropskou harmonizovanou normou poskytovat poskytovatelům předpoklad shody.

Poskytovatelé univerzálních modelů umělé inteligence by dále měli být schopni prokázat shodu pomocí alternativních vhodných prostředků, pokud nejsou k dispozici kodexy správné praxe nebo harmonizované normy nebo se rozhodnou na ně nespoléhat.

Obsahuje zákon o AI ustanovení týkající se ochrany životního prostředí a udržitelnosti?

Cílem návrhu AI je zabývat se riziky pro bezpečnost a základní práva, včetně základního práva na vysokou úroveň ochrany životního prostředí. Jedním z výslovně uvedených a chráněných právních zájmů je také životní prostředí.

Komise je požádána, aby požádala evropské normalizační organizace, aby vytvořily normalizační výstup týkající se procesů podávání zpráv a dokumentace s cílem zlepšit výkon zdrojů systémů umělé inteligence, jako je snížení spotřeby energie a jiných zdrojů vysoce rizikového systému umělé inteligence během jeho životního cyklu, a energeticky účinný vývoj univerzálních modelů umělé inteligence.

Kromě toho je Komise požádána, aby do dvou let po datu použitelnosti nařízení a poté každé čtyři roky předložila zprávu o přezkumu pokroku ve vývoji normalizačních výstupů v oblasti energeticky účinného vývoje modelů pro obecné použití a posoudila potřebu dalších opatření nebo akcí, včetně závazných opatření nebo akcí.

Kromě toho jsou poskytovatelé univerzálních modelů umělé inteligence, kteří jsou vyškoleni na velké objemy dat, a proto jsou náchylní k vysoké spotřebě energie, povinni zveřejňovat spotřebu energie. V případě obecných modelů umělé inteligence se systémovými riziky je dále třeba posoudit energetickou účinnost.

Komise je zmocněna vyvinout vhodnou a srovnatelnou metodiku měření pro tyto povinnosti zveřejňování.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Jak mohou nová pravidla podpořit inovace?

Regulační rámec může zvýšit zavádění umělé inteligence dvěma způsoby. Na jedné straně bude rostoucí důvěra uživatelů zvyšovat poptávku po AI využívané společnostmi a veřejnými orgány. Na druhé straně zvýšením právní jistoty a harmonizací pravidel získají poskytovatelé umělé inteligence přístup na větší trhy s produkty, které uživatelé a spotřebitelé oceňují a kupují. Pravidla se použijí pouze tam, kde je to nezbytně nutné, a způsobem, který minimalizuje zátěž pro hospodářské subjekty, s lehkou strukturou řízení.

Zákon o AI dále umožňuje vytváření regulačních sandboxů a testování v reálném světě, které poskytují řízené prostředí pro testování inovativních technologií po omezenou dobu, a tím podporují inovace společností, malých a středních podniků a začínajících podniků v souladu se zákonem o AI. Tato spolu s dalšími opatřeními, jako jsou další sítě center AI Excellence Center a partnerství veřejného a soukromého sektoru v oblasti umělé inteligence, dat a robotiky, a přístup robotiky, a digitálních robotiky, a testovacím a experimentálním zařízením pomohou společnostem vytvořit správné rámcové podmínky pro vývoj a nasazení umělé inteligence.

Testování vysoce rizikových systémů umělé inteligence v reálném světě lze provádět po dobu maximálně 6 měsíců (které lze prodloužit o dalších 6 měsíců). Před testováním je třeba vypracovat plán a předložit ho orgánu dozoru nad trhem, který musí plán a konkrétní testovací podmínky schválit, s výchozím tichým souhlasem, pokud do 30 dnů neodpoví. Testování může být předmětem neohlášených kontrol ze strany úřadu.

Testování v reálném světě lze provádět pouze za předpokladu specifických záruk, např. uživatelé systémů, které jsou testovány v reálném světě, musí poskytnout informovaný souhlas, testování na ně nesmí mít žádný negativní vliv, výsledky musí být vratné nebo nerespektovatelné a jejich data musí být po ukončení testování vymazána. Zvláštní ochrana má být poskytnuta zranitelným skupinám, tj. z důvodu jejich věku, tělesného nebo duševního postižení.

Jakou roli hraje Pakt o umělé inteligenci při provádění zákona o umělé inteligenci?
Pakt o umělé inteligenci, který inicioval komisař Breton v květnu 2023, si klade za cíl posílit zapojení mezi úřadem pro umělou inteligenci a organizacemi (I. pilíř) a podpořit dobrovolný závazek odvětví začít s prováděním požadavků zákona o umělé inteligenci před zákonem stanoveným termínem (II. pilíř).

Zejména v rámci Pilíře I budou účastníci přispívat k vytvoření spolupracující komunity, sdílet své zkušenosti a znalosti. To zahrnuje workshopy organizované Úřadem pro umělou inteligenci, které účastníkům umožní lépe porozumět zákonu o umělé inteligenci, jejich povinnostem a tomu, jak se připravit na jeho implementaci. Kancelář AI zase může shromažďovat poznatky o osvědčených postupech a výzvách, kterým účastníci čelí.

V rámci Pilíře II jsou organizace vyzývány, aby prostřednictvím dobrovolných závazků proaktivně zveřejňovaly procesy a postupy, které zavádějí, aby předvídaly dodržování předpisů. Závazky jsou zamýšleny jako „prohlášení o angažovanosti“ a budou obsahovat akce (plánované nebo probíhající) ke splnění některých požadavků zákona o AI.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034

Většina pravidel zákona o umělé inteligenci (například některé požadavky na vysoce rizikové systémy umělé inteligence) bude platit na konci přechodného období (tj. doby mezi vstupem v platnost a datem použitelnosti).

V této souvislosti a v rámci Paktu AI úřad AI vyzývá všechny organizace, aby proaktivně předjímaly a implementovaly některá klíčová ustanovení zákona o AI s cílem co nejdříve zmírnit rizika pro zdraví, bezpečnost a základní práva.

Více než 700 organizací již vyjádřilo svůj zájem připojit se k iniciativě Pakt AI v návaznosti na výzvu zahájenou v listopadu 2023. První informační schůzka se konala online dne 6. května a zúčastnilo se jí 300 účastníků. Oficiální podpis dobrovolných závazků je plánován na podzim 2024. V prvním zářijovém týdnu se bude konat workshop o Paktu AI.

Jaký je mezinárodní rozměr přístupu EU?

AI má důsledky a výzvy, které přesahují hranice; proto je důležitá mezinárodní spolupráce. Kancelář AI má na starosti mezinárodní angažmá Evropské unie v oblasti AI na základě zákona o AI a Koordinovaného plánu pro AI. EU se snaží podporovat odpovědné vedení a řádnou správu AI ve spolupráci s mezinárodními partnery a v souladu s mnohostranným systémem založeným na pravidlech a hodnotami, které zastává.

EU se bilaterálně i multilaterálně zapojuje do podpory důvěryhodné, na člověka zaměřené a etické umělé inteligence. V důsledku toho je EU zapojena do mnohostranných fór, kde se diskutuje o umělé inteligenci – zejména G7, G20, OECD, Rada Evropy, Globální partnerství pro umělou inteligenci a OSN – a EU má úzké dvoustranné vazby např. s Kanadou, USA, Indií, Japonskem, Jižní Koreou, Singapurem a regionem Latinské Ameriky a Karibiku.

Dokument připravil: Miroslav Kalinský, Hlavní GDPR konzultant a DPO
EVERY REGARD s.r.o., Ostrava - Slezská Ostrava, Zámostní 1155/27, PSČ 710 00, IČO: 05460034