12. 6. 2026

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

Posouzení shody dle AI Act - zkušenosti z praxe

Tento odborný článek poskytuje ucelený pohled na proces posouzení shody v kontextu nařízení (EU) 2024/1689 (AI Act). Text se věnuje klasifikaci systémů umělé inteligence do jednotlivých kategorií rizik, od striktně zakázaných praktik až po specifické povinnosti modelů pro obecné účely (GPAI). Jádrem článku je detailní rozbor praktických kroků nezbytných pro splnění regulatorních požadavků, včetně sestavení technické dokumentace, implementace systému řízení kvality a hodnocení dopadů na základní práva. Autorka článku má zkušenosti z praxe advokátní kanceláře s posouzením shody konkrétního softwaru s prvky AI, jeho posuzování během vývojové fáze, zkušební fáze i uvedení do praxe, a proto nabízí nejen praktická, ale i konkrétní metodická doporučení a praktické tipy pro integraci těchto pravidel do praxe poskytovatelů systémů s prvky AI i s ohledem na provázání s ochranou osobních údajů. Autorka článku se specializuje na GDPR a posouzení shody dle AI Act.

AI Act - úvod do nové éry regulace

AI Act neboli nařízení (EU) 2024/1689[1] asi již netřeba představovat vzhledem k tomu, že tady s námi umělá inteligence je a taky bude a toto nařízení jí dává hranice v rámci prostoru EU. Na rozdíl od předchozích sektorových regulací zavádí AI Act komplexnější rámec, který se dotýká každého subjektu vyvíjejícího nebo využívajícího systémy umělé inteligence v Unii. Jádrem celého nařízení je tzv. **posouzení shody** (*conformity assessment*), které neslouží pouze jako administrativní povinnost, ale jako základní mechanismus pro zajištění bezpečnosti, transparentnosti a důsledného dodržování základních práv občanů EU. Tato regulace reaguje na rychlý technologický vývoj a snaží se nastavit jasná pravidla hry, která podpoří inovace při současném omezení rizik. Vzhledem k tomu, že jsme v naší advokátní kanceláři měli tu profesní čest podílet se jako odborníci se specializací na GDPR právě na posouzení shody s AI Act u konkrétních softwarů využívajícíCH prvky AI, a to od počáteční fáze, přes spolupráci s vývojáři, testovací fázi až po uvedení softwaru do praxe, ráda bych se po úvodním shrnutí kategorií systémů věnovala v článku i doporučením na základě našich zkušeností pro praxi.

Kategorizace systémů podle míry rizika

Akt o AI opouští binární vidění světa a zavádí stupňovitou regulaci založenou na míře rizika, které daný systém představuje pro zdraví, bezpečnost nebo základní práva fyzických osob.

1. **Zakázané systémy (Nepřijatelné riziko):** Článek 5 nařízení definuje praktiky, které jsou v EU nepřípustné. Patří sem systémy využívající podprahové techniky k manipulaci chování, sociální skóring prováděný veřejnými orgány nebo systémy biometrické identifikace v reálném čase pro účely vymáhání práva na veřejných místech (s výjimkou specifických výjimek)[2]. U těchto systémů je jakákoliv forma posouzení shody irelevantní, neboť jejich provozování je zakázáno.
2. **Vysoce rizikové systémy (High-risk):** Tato kategorie tvoří těžiště regulace. Zahrnuje systémy používané v kritické infrastruktuře, vzdělávání, náboru zaměstnanců, hodnocení úvěruschopnosti nebo při vymáhání práva (dle Přílohy III). Tyto systémy podléhají

nejpřísnějšímu režimu posouzení shody.[3]

3. **Systémy s omezeným rizikem (Transparentnost):** U systémů, jako jsou chatboti, systémy pro rozpoznávání emocí nebo generátory „deepfakes“, se posouzení shody zaměřuje primárně na informační povinnost. Uživatel musí být jasně informován, že komunikuje s AI (článek 50).[4]
4. **Modely pro obecné účely (GPAI):** Specifická pravidla platí pro modely, jako jsou velké jazykové modely (LLM). Pokud tyto modely vykazují systémové riziko (dané např. výpočetní kapacitou použitou k trénování), podléhají povinnostem v oblasti hodnocení modelů, testování a hlášení incidentů.[5]

Proces posouzení shody v praxi

Posouzení shody u vysoce rizikových systémů je komplexní proces, který musí být dokončen před uvedením systému na trh nebo do provozu. Posouzení se musí provést v případě všech systémů, které zamýšlejí prvky AI použít a na prvním místě je potřeba zařadit systém do správné kategorie (viz výše). V praxi jsme se již setkali s tím, že do poslední chvíle nebylo jasné, zda bude systém spadat do vysoce rizikové kategorie, nebo „pouze“ do kategorie „systém s omezeným rizikem“, protože se náš právní tým podílel na celém procesu i během vývoje. Je tedy důležité si uvědomit, že při intenzivní spolupráci v týmu lze ve výsledku díky aplikaci správných nástrojů dojít do bodu, kdy z původně zamýšleného systému v kategorii vysoce rizikové lze nastavit systém tak, že zákazník dojde k cíli, který na začátku požadoval, aniž by přitom zasahoval do oblasti ochrany osobních údajů. I z tohoto důvodu doporučujeme intenzivní spolupráci na projektech při vývoji softwarů dle zadání zákazníka zapojit specialistu či právníka do procesu od začátku a hledat postupy a cesty společně.

V praxi v případě vysoce rizikových systémů bych ráda zdůraznila následující klíčové pilíře:

- **Sestavení technické dokumentace (Příloha IV):** Tato dokumentace musí poskytovat veškeré informace nezbytné k posouzení souladu systému s požadavky. Musí obsahovat obecný popis systému, podrobný popis prvků systému a procesu jeho vývoje (včetně metodik a použitých dat), popis systému řízení rizik a výsledky validace a testování[6]. Dokumentace musí být uchovávána po dobu deseti let od uvedení systému na trh.
- **Zavedení systému řízení kvality (QMS):** Poskytovatelé vysoce rizikových systémů musí zavést zdokumentovaný systém řízení kvality (článek 17). Ten pokrývá strategii dodržování souladu s nařízením, postupy správy dat, technické normy, testování a kontrolu kvality. V praxi se jako nejvhodnější jeví integrace s mezinárodní normou ISO/IEC 42001.
- **Hodnocení dopadů na základní práva (FRIA):** Určení nasazovatelé (zejména orgány veřejné moci nebo subjekty poskytující služby veřejného zájmu) musí před nasazením vysoce rizikového systému provést posouzení dopadů na základní práva (článek 27).[7] Toto hodnocení musí specifikovat účel použití, dobu trvání nasazení a kategorie osob, které mohou být systémem ovlivněny.
- **Monitoring po uvedení na trh:** Povinnosti nekončí schválením systému. Poskytovatelé musí zavést systém sledování po uvedení na trh (článek 61), který bude systematicky shromažďovat a vyhodnocovat data o výkonnosti systému a identifikovat případné neočekávané incidenty nebo rizika.

Praktické tipy pro implementaci

1. **AI Mapping a včasná klasifikace:** Organizace by měly začít auditováním všech využívaných softwarových nástrojů. Často jsou prvky AI integrovány v běžných podnikových systémech (např. automatizované třídění životopisů), které mohou spadat do vysoce rizikové kategorie.
2. **Využití synergií s GDPR:** Mnoho požadavků Aktu o AI (např. správa dat, transparentnost,

DPIA) se překrývá s povinnostmi podle GDPR. To není žádným překvapením vzhledem k tomu, že se v odborných kruzích často mluví o AI Act jako o GDPR v novém kabátě rozšířeném o detailnější zaměření na technickou dokumentaci. Což ale ani pro oblast GDPR není žádnou novinkou. Doporučuje se integrovat posouzení shody do stávajících procesů ochrany osobních údajů, čímž se sníží administrativní zátěž a nejen to. Dobře nastavené procesy u GDPR můžou naopak napomoci snadnějšímu uvedení systému s AI do praxe, protože se již funkční systémy pro GDPR rozšíří o další kategorii.

3. **Governance a mezioborové týmy:** Praxe ukazuje, že posouzení shody není pouze právní či technický úkol – pro správné posouzení je potřeba aktivovat celý tým odborníků, není možné vynechat vývojáře nebo naopak obchodní zástupce, či nepředat všechny podklady externímu právníkovi. Klíčové je zde vytvořit tým, který se navzájem pravidelně informuje, a výsledné nebo i rozpracované návrhy textu posouzení by měly projít kontrolou každého z týmu. Tzn. samotné posouzení vyžaduje úzkou spolupráci IT oddělení (*data scientists*), právníků (*compliance*) a zástupců byznysu (*owners of use-cases*). Dalším doporučením je zapojení všech osob z týmu do celého procesu již od začátku vývoje, protože to šetří ve výsledku čas i náklady, kdy právník může včas odhalit riziková místa a vývojář tak může hned hledat vhodnější řešení.
4. **Smluvní zajištění dodavatelského řetězce:** Pokud organizace AI systém pouze nakupuje, musí si od dodavatele smluvně zajistit přístup k technické dokumentaci a záruku, že systém prošel řádným posouzením shody. Praxe ukazuje, že je aktuálně toto velkým problémem, pokud nakupujete od poskytovatelů mimo EU, kterých je aktuálně drtivá většina a zároveň jsou ve vývoji napřed právě proto, že nejsou „omezeni“ právní regulací EU. Na druhou stranu je ale potřeba vnímat, že EU chrání základní hodnoty a použití mimoevropských systémů je pro nasazovatele potenciálně velmi rizikové. Takže se v praxi více osvědčuje volit evropské dodavatele, kteří plní požadavky EU a jsou schopni doložit technickou dokumentaci i záruky. Odpovědnost za nasazení v souladu s určeným účelem nese nasazovatel. Toto je důležitý bod, který se v praxi často opomíjí a opět je zde důležité, aby nasazovatel o této povinnosti věděl, popřípadě ji na to upozornil právní zástupce.

Závěrem

Posouzení shody podle AI Act představuje nový standard odpovědnosti v digitálním věku, který zároveň vyžaduje zapojení více odborníků než pouze právníka nebo pouze odborníka na IT, a to pokud možno od prvotní myšlenky až po zavedení do praxe. Ačkoliv s sebou přináší zvýšené náklady na vývoj a compliance, je nezbytným krokem k budování důvěry v technologie umělé inteligence. Dále je dobré nevnímat AI Act jako prvek omezující svobodu trhu a zbavit se předpojatosti ve smyslu „mimoevropský trh má business výhodu v tom, že není regulován“, protože takové uvažování je krátkozraké a taky nebezpečné. AI Act chrání základní práva občanů EU právě důrazem na požadavek posouzení a následné doložení včetně záruk a technických dat, což dále buduje i důvěru v moderní technologie ze strany veřejnosti a její ochotu tyto technologie nechat zasahovat v podobě různých produktů do jejich každodenního života. Pro podniky, které proces uchopí strategicky a včas, se schopnost prokázat shodu s evropskými standardy stane významnou konkurenční výhodou na globálním trhu. Transparentní a bezpečná AI není pouze regulatorním požadavkem, ale etickým imperativem moderní společnosti.

Mgr. Kristína Udržalová,
právník a specialista na GDPR

PADĚRA & PARTNEŘI s.r.o. advokátní kancelář

Svaté Anežky České 32
530 02 Pardubice

Tel.: + 420 773 240 555
E-mail: info@akprp.cz

---

[1] Nařízení Evropského parlamentu a Rady (EU) 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci (Akt o umělé inteligenci)

[2] Srovnej Článek 5 odst. 1 písm. a) a b) Nařízení (EU) 2024/1689 o zakázaných praktikách

[3] Klasifikace vysoce rizikových systémů je upravena v Článku 6 a podrobněji rozvedena v Příloze III (Annex III)

[4] Povinnosti týkající se transparentnosti pro určité systémy AI dle Článku 50 Nařízení

[5] Definice a povinnosti modelů GPAI (General-Purpose AI) jsou obsaženy v Hlavě V (Článek 51 a násl.)

[6] Podrobné požadavky na obsah technické dokumentace stanoví Příloha IV (Annex IV) Nařízení

[7] Článek 27 Nařízení (EU) 2024/1689 – Posouzení vlivu na základní práva u vysoce rizikových systémů AI.

Další články:

- Nový zákon o veřejných dražbách, aukce a obálkové metody
- Pohled přes hranice – natáčení pornografických klipů jako důvod výpovědi z nájmu bytu
- Nařízení EU o umělé inteligenci a jeho dopady na využití jazykových modelů v advokátní praxi
- Revize zájezdové směrnice: co přináší, co hrozilo a co to znamená pro praxi
- Kupní smlouva o převodu nemovitosti bez uvedení výše kupní ceny
- Druhá „tlačítková novela": povinné tlačítko pro odstoupení od smlouvy
- Souhlas s veřejným užíváním pozemku jako překážka nároku na bezdůvodné obohacení – nález Ústavního soudu sp. zn. I. ÚS 2541/25

- Kupní smlouva bez přesného určení kupní ceny
- Byznys a paragrafy, díl 36.: Doložka o mlčenlivosti
- Detekce podezřelého obchodu v kontextu hazardních her
- AI omnibus