IUSTORIA
Advokátní kancelář

telefon: (+420) **777 366 857**
email: info@iustoria.cz
web: www.iustoria.cz

1. Klíčové a nepřenositelné povinnosti pro zavádějící subjekty

Ačkoliv hlavní tíha regulace dopadá na vývojáře (poskytovatele) AI systémů, zavádějící subjekty (firmy, které systémy nasazují a využívají) mají vlastní okruh povinností, zejména pokud používají systémy klasifikované jako **vysoce rizikové**.

Povinnosti u vysoce rizikových systémů:

Mezi klíčové povinnosti firem, které používají vysoce rizikové systémy (např. v náboru zaměstnanců, hodnocení úvěrového rizika nebo v kritické infrastruktuře), patří:

- **Zajištění efektivního lidského dohledu:** Firmy musí zajistit, že vysoce rizikové AI systémy budou pod **efektivním lidským dohledem**. Personál musí mít odpovídající odbornou způsobilost k interpretaci výstupů, identifikaci anomálií a k zásahu nebo zastavení systému v případě potřeby.
- **Používání v souladu s pokyny:** Systém musí být používán přesně podle dokumentace a instrukcí dodaných poskytovatelem.
- **Vedení záznamů (Logů):** Je povinné uchovávat automaticky generované záznamy o činnosti systému, což slouží ke sledování a kontrole.
- **Transparentnost a informovanost:** Firma musí informovat dotčené osoby (např. zaměstnance nebo zákazníky), že jsou vystaveny rozhodování nebo interakci s AI systémem.
- **Posouzení dopadu na základní práva (FRIA):** V určitých případech (zejména u veřejných subjektů nebo soukromých firem poskytujících veřejné služby) je nutné provést posouzení dopadu nasazení systému na základní práva.
- **Ohlašovací povinnost:** Pokud firma zjistí, že AI systém představuje vážné riziko nebo došlo k incidentu, musí **neprodleně informovat poskytovatele a příslušné vnitrostátní orgány**.
- **Odpovědnost za data:** Zavádějící subjekt odpovídá za **kvalitu a relevanci dat**, kterými je systém "krmen". Pokud firma použije nevhodná, zkreslená nebo diskriminační data, ponese odpovědnost za chybné a potenciálně škodlivé výstupy AI.
- **AI gramotnost zaměstnanců:** Firmy musí zajistit, aby jejich zaměstnanci měli dostatečné **povědomí o fungování, příležitostech a rizicích** těchto systémů. Tato povinnost vstoupila v platnost již v únoru 2025.

2. Dopady na malé a střední firmy (SME) a riziko regulace

Pro drtivou většinu českých SME (řemeslníci, účetní, marketingové agentury) AI Act **nepředstavuje nepřekonatelnou byrokratickou zátěž**, protože jejich používané nástroje spadají do kategorií minimálního nebo omezeného rizika.

Rizikové kategorie pro SME:

Kategorie rizika	Příklady AI nástrojů	Povinnosti dle AI Act
Minimální riziko	Spamové filtry, AI pro automatické zaúčtování faktur, optimalizace skladových zásob, asistenti pro psaní kódu.	**Žádné nové zákonné povinnosti**. Stále platí obecná odpovědnost za výsledek práce (např. za správnost účetnictví).
Omezené riziko	Chatboti pro zákaznickou komunikaci, nástroje pro generování obsahu (text, video, realistické obrázky/deepfakes).	**Jednoduchá informační povinnost (transparentnost).** Firma musí zajistit, aby bylo zřejmé, že uživatel komunikuje se strojem, nebo že obsah byl generován AI.
Vysoce rizikové	Samostatný AI software pro předvýběr kandidátů na pracovní pozice (HR).	**Plná paleta povinností** (lidský dohled, vedení záznamů, posouzení rizik).

Kritický scénář pro drobného podnikatele (HR past):

Použití obecného nástroje, jako je **ChatGPT (nebo Gemini), pro vyhodnocení životopisů** několika zájemců o práci, způsobí, že i drobný podnikatel se stává **"zavádějícím subjektem" vysoce rizikového systému**.

- **Důvod:** Systémy AI používané pro nábor, výběr, hodnocení nebo rozhodování o pracovním poměru jsou **explicitně definovány jako vysoce rizikové**, protože mají dopad na základní práva.
- **Nutná opatření:** Podnikatel musí zajistit **absolutní lidský dohled**; výstup z AI **nesmí být konečným rozhodnutím**. Doporučuje se ověřovat přesnost a eliminovat zkreslení (bias) v datech, archivovat záznamy (prompty a odpovědi) a ideálně informovat kandidáty o použití AI pro asistenci.
- **Riziko porušení a odhalení:** Riziko porušení povinnosti lidského dohledu je **velmi vysoké** pro neznalé podnikatele. Riziko odhalení je sice v současné době nízké, ale s rostoucím potenciálem, zejména prostřednictvím **stížností od neúspěšných kandidátů**.

3. Zvýšení rizika při automatizaci (Make, Zapier)

Zapojení automatizačních platforem (Make, Zapier, Relay) do AI pracovních postupů slouží jako **multiplikátor rizika**, protože mění AI z asistenta na **autonomního vykonavatele**.

- **Ztráta dohledu:** Pokud automatizovaný scénář (např. v HR nebo cenotvorbě) provede úkon, který má dopad na práva lidí (např. automatické odeslání zamítavého e-mailu kandidátovi, jehož skóre v AI bylo nízké), dochází k **závažnému porušení klíčové povinnosti AI Actu – ztrátě efektivního lidského dohledu**.
- **Doporučený přístup:** Bezpečné používání vyžaduje, aby automatizace fungovala v režimu **„Člověk ve smyčce“ (Human in the Loop)**. Poslední krok automatizovaného workflow (např. v Make/Zapieru) nesmí být „proveď finální akci“, ale vždy **„předat ke schválení člověku“**.

4. Finanční hrozby a sankce

Ignorování povinností AI Actu může mít pro firmy, včetně malých a středních podniků, **citelné a likvidační finanční dopady**.

- **Za nedodržení povinností u vysoce rizikových systémů** hrozí pokuta **až 15 milionů eur nebo 3 % z celosvětového ročního obratu** (podle toho, co je vyšší).
- Pro malé podnikatele by i mírnější, úměrná pokuta mohla dosáhnout **likvidační částky v řádu desítek až stovek tisíc korun**.
- Kromě přímých pokut hrozí i riziko **žalob od neúspěšných kandidátů** podle antidiskriminačního zákona, kde by důkazní břemeno leželo na podnikateli.

5. Role dozorových orgánů v ČR

Kontrola dodržování povinností AI Actu bude v České republice probíhat na několika úrovních a zahrnuje kombinaci proaktivního dohledu a reaktivního šetření.

- **Kdo kontroluje:** Hlavním orgánem dozoru nad trhem bude **Český telekomunikační úřad (ČTÚ)**, který má pravomoc provádět kontroly a ukládat sankce.
- **Jak se zjistí porušení:** Porušení se odhalí především prostřednictvím **hlášení vážných incidentů**, **aktivním monitorováním trhu** ze strany úřadů a **podněty a stížnostmi třetích stran** (např. od spotřebitelů nebo neúspěšných kandidátů).
- **Vážný incident:** Je definován jako porucha nebo neočekávané chování AI systému, které vede, nebo by mohlo vést, k závažným negativním následkům, jako je **smrt, vážné poškození zdraví, závažné narušení kritické infrastruktury, nebo porušení základních práv**. Zavádějící subjekt má povinnost incident nahlásit poskytovateli a úřadům neprodleně, nejpozději do 15 dnů od zjištění.

6. Dopady souběžné regulace (GDPR a únik dat)

Na rizika úniku dat firem se AI Act nezaměřuje primárně, ale řeší je **silné a zavedené normy**, jejichž povinnosti se při používání AI sčítají.

- **GDPR (Osobní údaje):** Chrání osobní údaje. Firma poruší GDPR, pokud zaměstnanec zkopíruje data zákazníků do **nezabezpečené bezplatné verze AI**, protože je předává třetí straně bez smluvního zajištění (DPA).
- **Zákon o ochraně obchodního tajemství (Firemní Know-how):** Chrání citlivé firemní údaje, jako jsou cenové strategie nebo zdrojové kódy. Nahrání unikátních technických výkresů do veřejné AI platformy představuje porušení obchodního tajemství a obrovskou ztrátu kontroly nad duševním vlastnictvím.

AI Act v tomto kontextu nepřímo přispívá k ochraně dat tím, že požaduje, aby vysoce rizikové systémy AI byly **robustní a odolné vůči kybernetickým útokům**, čímž se snaží zabránit tomu, aby útok vedl k selhání AI a způsobení škody.

Závěrem, české firmy musí k AI Actu přistupovat **proaktivně** a chápat ho jako **strategický rámec** pro bezpečné zavádění inovací. To zahrnuje provedení inventury a klasifikace AI systémů a vytvoření interních pravidel (AI Governance), což přesahuje rámec pouhého produktového školení od dodavatele.