Ambit

www.ambit.law

PRAKTICKÝ PRŮVODCE PRO SPOLEČNOSTI

AI Act v praxi

Přehled nejdůležitějších povinností pro společnosti

Praktický průvodce pro společnosti, které vyvíjejí, dodávají nebo používají systémy umělé inteligence.

NAŘÍZENÍ (EU)

2024/1689 · Akt o umělé inteligenci

13 KAPITOL

Role, rizika a praktická příprava

ČERVEN 2026

Obsah

Třináct kapitol od základní orientace v regulaci až po praktickou cestu k souladu.

01 Úvodní slovo 03

02 Co AI Act reguluje 04

03 Koho se AI Act týká 05

04 Zakázané praktiky 06

05 Vysoce rizikové systémy AI 07

06 Obecné modely AI (GPAI) 11

07 Povinnosti transparentnosti 13

08 Časová osa použitelnosti 16

09 Česká implementace 17

10 GDPR a navazující regulace 17

11 Compliance v šesti krocích 18

12 Jak vám pomůžeme 19

13 Závěr 20

01 Úvodní slovo

Umělá inteligence (AI) se rychle přesouvá z experimentální fáze do každodenního provozu organizací. Používá se v marketingu, HR, zákaznické podpoře, finančních službách, zdravotnictví, výrobě, veřejné správě i při interním rozhodování. Spolu s tím roste i právní odpovědnost organizací, které systémy AI vyvíjejí, dodávají nebo používají.

Evropská unie (EU) proto přijala nařízení Evropského parlamentu a Rady (EU) 2024/1689, známé jako Akt o umělé inteligenci nebo AI Act, první komplexní unijní právní rámec pro umělou inteligenci. Akt je přímo použitelný ve všech členských státech EU, ale úprava jeho praktického vymáhání bude doplněna vnitrostátními pravidly, zejména pokud jde o určení orgánů dozoru, procesní otázky a sankční mechanismy.

Akt o umělé inteligenci se neuplatní izolovaně. V praxi se bude prolínat zejména s GDPR, regulací kyberbezpečnosti, ochranou spotřebitele, pracovním právem, právem duševního vlastnictví, sektorovou regulací a připravovanou českou adaptační legislativou.

Cílem tohoto handbooku je poskytnout klientům základní orientaci v tom, kdy se Akt o umělé inteligenci použije, jaké role rozlišuje, jaká rizika reguluje a jak se na nová pravidla prakticky připravit.

O AUTOROVI



Jaroslav Menčík

partner · Ambit

Jaroslav se v právu pohybuje přes patnáct let a specializuje se na právo informačních technologií, duševní vlastnictví a venture kapitálové a M&A transakce. Vyjednal přes 150 VC a M&A transakcí v České republice i ve středoevropském regionu. Vedle právního vzdělání z ČR a USA (New York University School of Law, Hauser Global Scholar) má i inženýrský titul z ekonomie; své znalosti pravidelně sdílí přednáškami na univerzitách a konferencích.

IT & TECHNOLOGIE · DUŠEVNÍ VLASTNICTVÍ · VC & M&A

KONTAKT:

jaroslav.mencik@ambit.law

02 Co AI Act reguluje

AI Act stanoví jednotná pravidla pro uvádění systémů AI na trh, jejich provoz a používání v EU. Stojí na jednoduché logice: **čím větší dopad může systém mít na práva, bezpečnost nebo zdraví lidí, tím přísnější pravidla se na něj vztahují.**

Zakázané postupy v oblasti AI	Úplný zákaz	kapitola 4 →
Vysoce rizikové systémy AI	Přísné povinnosti	kapitola 5 →
Obecné modely AI (GPAI)	Mírnější režim	kapitola 6 →
Povinnosti transparentnosti	Informační povinnost	kapitola 7 →

AI Act zároveň zavádí **regulační sandboxy**: kontrolované prostředí, kde lze inovativní systémy vyvíjet, trénovat a testovat ještě před uvedením na trh, včetně testování v reálných podmínkách pod dohledem.

Dále upravuje zejména zřízení Evropské rady pro umělou inteligenci a poradního fóra, které poskytuje technické odborné znalosti radě a Evropské komisi. Věnuje se také určení příslušných vnitrostátních orgánů a jednotného kontaktního místa, jakož i dozoru nad trhem a kontrole systémů AI na trhu EU.

03 Koho se AI Act týká

AI Act nedopadá pouze na velké technologické společnosti. Týká se každé organizace, která systém AI vyvíjí, uvádí na trh, integruje do produktu, používá při své činnosti, dováží nebo distribuuje.

Rozhoduje vaše role, a často jich máte víc najednou.

KLÍČOVÉ ROLE

ROLE	DEFINICE
Poskytovatel (provider)	Vyvíjí systém AI (nebo ho nechává vyvíjet) a uvádí ho na trh či do provozu pod svým jménem, za úplatu i zdarma.
Zavádějící subjekt (deployer)	Používá systém AI v rámci své činnosti. Nejčastější role běžných společností.
Dovozce	Uvádí na trh EU systém AI od subjektu ze třetí země.
Distributor	Subjekt v dodavatelském řetězci (jiný než poskytovatel či dovozce), který dodává systém AI na trh EU.
Výrobce produktu s AI	Uvádí na trh produkt se zabudovaným systémem AI pod svým jménem.
Zplnomocněný zástupce	Subjekt v EU pověřený plnit povinnosti za poskytovatele ze třetí země.

MIMO EU? STEJNĚ TO PLATÍ

AI Act dopadá i na poskytovatele a zavádějící subjekty mimo EU, pokud je **výstup jejich systému používán v EU**. Zeměpisná poloha není určující.

04 Zakázané praktiky

Některé způsoby použití AI jsou natolik rizikové, že je AI Act zakazuje úplně, bez ohledu na roli nebo souhlas dotčených osob. Zákazy platí už **od 2. února 2025** a jejich porušení je sankcionováno nejpřísněji: pokuty až **35 mil. EUR nebo 7 % celosvětového obratu**.

1 **Manipulativní a podprahové techniky**

Systémy, které podprahově nebo klamavě ovlivňují chování a způsobují (či mohou způsobit) podstatnou újmu.

2 **Zneužití zranitelnosti**

Cílení na zranitelnost danou věkem, zdravotním postižením nebo sociálně-ekonomickou situací.

3 **Sociální skórování**

Hodnocení lidí podle chování či vlastností vedoucí k neoprávněnému nebo nepřiměřenému znevýhodnění.

4 **Predikce trestné činnosti**

Posouzení rizika spáchání trestného činu výhradně na základě profilování nebo osobnostních rysů.

5 **Necílené získávání podob obličejů**

Hromadné stahování snímků z internetu nebo kamer za účelem budování databází rozpoznávání obličejů.

6 **Rozpoznávání emocí na pracovišti a ve školství**

S výjimkou zdravotních a bezpečnostních důvodů.

7 **Biometrická kategorizace**

Odvozování rasy, politických názorů, náboženství či sexuální orientace z biometrických údajů.

8 **Biometrická identifikace na dálku v reálném čase**

Ve veřejně přístupných prostorech pro účely vymáhání práva, až na úzce vymezené výjimky.

9 **Generování nelegálního sexuálního obsahu**

Materiál zobrazující zneužívání dětí či intimní obsah identifikovatelných osob bez souhlasu (zákaz od 2. 12. 2026).

NEJVYŠŠÍ SANKCE

35 mil. €

nebo 7 % celosvětového obratu, podle toho, co je vyšší (u MSP a start-upů nižší z hodnot).

PRAKTICKÝ DOPAD

I běžné marketingové, HR nebo bezpečnostní nástroje se mohou nečekaně přiblížit zakázané praktice. Hranici je třeba posoudit dřív, než nástroj nasadíte.

05 Vysoce rizikové systémy AI

Tady leží těžiště celé regulace. Vysoce rizikové systémy („VRS“) nesou nejvíce povinností a dopadají hlavně na poskytovatele, zavádějící subjekty a dovozce. Prvním krokem je správně poznat, zda váš systém do této kategorie spadá.

KDY JE SYSTÉM VYSOCE RIZIKOVÝ: DVĚ CESTY (ČL. 6)

Příloha I

Bezpečnostní komponenta produktu

Systém je bezpečnostní komponentou produktu (nebo sám produktem) podle harmonizačních předpisů EU a musí projít posouzením shody třetí stranou, např. zdravotnické prostředky, stroje, hračky.

Příloha III

Citlivá oblast použití

Systém se používá v citlivé oblasti: biometrie, kritická infrastruktura, vzdělávání, zaměstnávání a řízení pracovníků, přístup k základním službám (úvěry, pojištění, dávky), vymáhání práva, migrace a azyl, výkon spravedlnosti a demokratické procesy.

PŘÍKLADY SYSTÉMŮ PODLE PŘÍLOHY III

- **Biometrická identifikace na dálku**
  s výjimkou systémů sloužících pouze k ověření totožnosti konkrétní osoby.
- **Rozpoznávání emocí**
  systémy určené k rozpoznávání emocí fyzických osob.
- **Kritická infrastruktura**
  bezpečnostní komponenty řízení dopravy nebo dodávek vody, plynu, topení a elektřiny.
- **Nábor a výběr zaměstnanců**
  cílené nabídky práce, třídění žádostí o zaměstnání a hodnocení uchazečů.
- **Úvěruschopnost**
  hodnocení a úvěrové bodování fyzických osob, s výjimkou odhalování finančních podvodů.

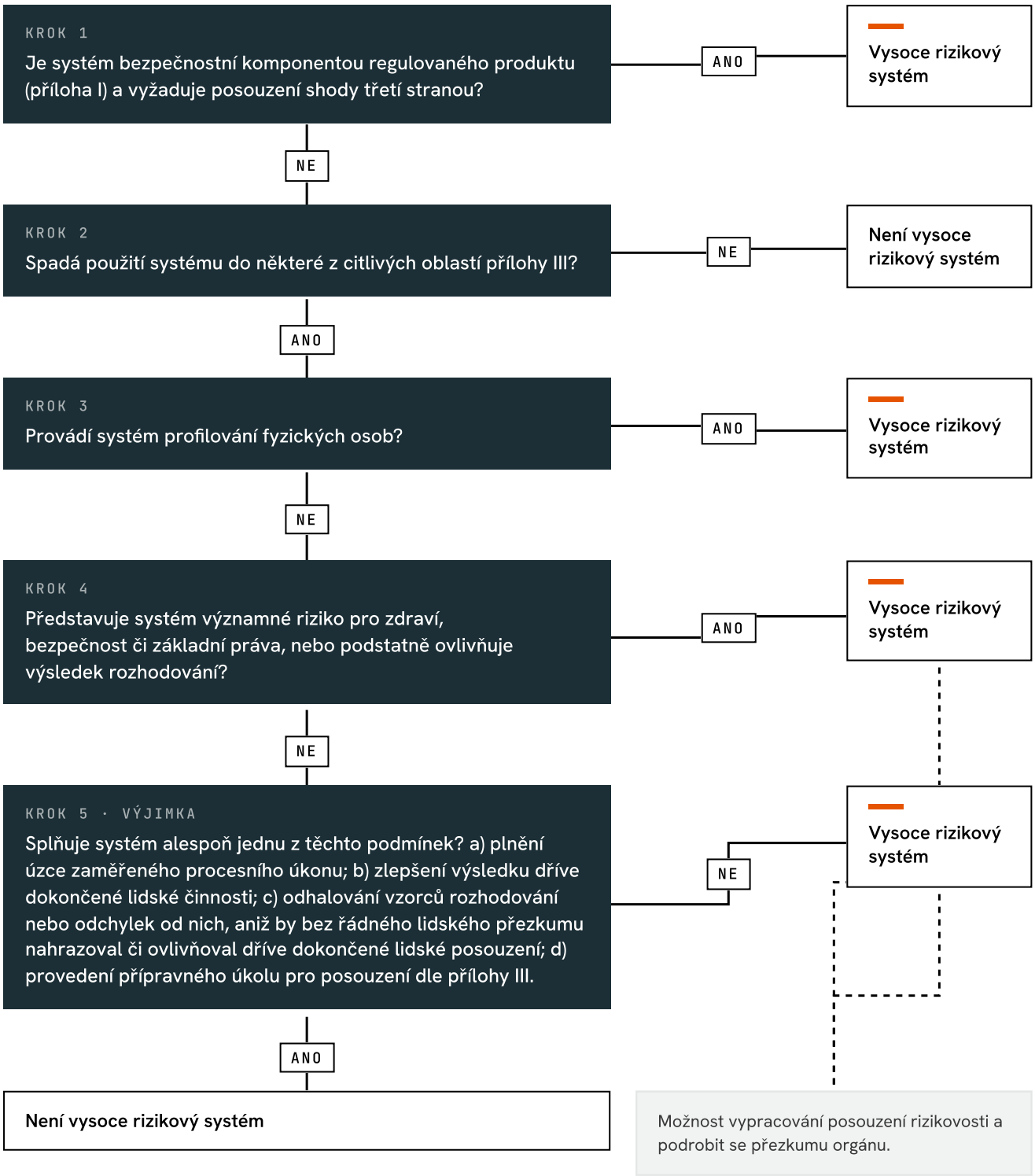
ROZHODOVACÍ SCHÉMA

Následující schéma vám pomůže systém předběžně zařadit. Postupujte odshora dolů.

str. 08 →

Je váš systém vysoce rizikový?

Předběžné zařazení podle čl. 6. Odpovídejte postupně odshora dolů; jakmile dojdete k výsledku, větev končí.



Povinnosti poskytovatelů VRS

Poskytovatel vysoce rizikového systému nese nejtěžší část povinností. Musí zejména:

1 **Zajistit soulad s požadavky na VRS**
Řídit rizika, spravovat data, vypracovat technickou dokumentaci, generovat protokoly, poskytnout návod, zajistit lidský dohled, přesnost i kyberbezpečnost.

2 **Uvést identifikaci na systému**
Uvést jméno, název či ochrannou známku a kontaktní adresu na systému, obalu nebo v dokumentaci.

3 **Zavést systém řízení kvality (QMS)**
Vytvořit a udržovat funkční systém řízení kvality (Quality Management System).

4 **Vést dokumentaci**
Technickou a QMS dokumentaci, rozhodnutí oznámených subjektů a EU prohlášení o shodě.

5 **Zajistit generování protokolů**
Automatické generování protokolů, je-li systém pod kontrolou poskytovatele.

6 **Provést posouzení shody**
Před uvedením na trh nebo do provozu.

7 **Vypracovat EU prohlášení o shodě**
A uchovávat jej.

8 **Umístit označení CE**
Na systém, obal či do dokumentace.

9 **Zaregistrovat systém v databázi EU**
Sebe i systém; i ten vyhodnocený jako nerizikový.

10 **Přijmout nápravná opatření**
Při nesouladu systému a poskytnout informace.

11 **Prokázat soulad**
Na žádost příslušného vnitrostátního orgánu.

12 **Zajistit přístupnost**
Dle směrnic (EU) 2016/2102 a (EU) 2019/882.

13 **Monitorovat systém po uvedení na trh**
Zavést, zdokumentovat a sestavit plán monitorování.

14 **Hlásit incidenty**
Závažné incidenty hlásit orgánům dozoru nad trhem.

15 **Poskytnout přístup k dokumentaci a datům**
Orgánům dozoru nad trhem: trénovací, validační a testovací data.

16 **Poskytnout přístup ke zdrojovému kódu**
Na odůvodněnou žádost orgánům dozoru nad trhem.

LHŮTA

Od 2. 8. 2026 (příloha I: od 2. 8. 2027). Novela AI Omnibus počítá s odkladem do 2. 12. 2027 (příloha III) a 2. 8. 2028 (příloha I).

SANKCE

Až **15 mil. EUR** nebo **3 % celosvětového obratu**, podle toho, co je vyšší (u MSP a start-upů nižší z hodnot).

Poskytovatelé usazení mimo EU musí před dodáním VRS na trh EU písemně jmenovat zplnomocněného zástupce usazeného v EU, na nějž se orgány obracejí ve všech otázkách souladu.

Povinnosti zavádějících subjektů VRS

Zavádějící subjekt (deployer) je nejčastější rolí běžných společností. Musí zejména:

1 **Přijmout technická a organizační opatření**
Aby byl systém používán v souladu s návodem.

2 **Zajistit lidský dohled**
Efektivně dohlížet na provoz systému.

3 **Zajistit kvalitu vstupních dat**
Zajistit jejich relevantnost a reprezentativnost.

4 **Monitorovat provoz**
Sledovat provoz a informovat poskytovatele o vzniklém riziku.

5 **Uchovávat protokoly**
Protokoly automaticky generované systémem.

6 **Informovat zaměstnance**
Před nasazením na pracovišti informovat zástupce a dotčené pracovníky.

7 **Informovat dotčené osoby**
O nichž systém rozhoduje nebo pomáhá rozhodovat.

8 **Provést posouzení dopadu (FRIA)**
Ve vymezených případech (zejm. banky a pojišťovny).

FRIA: posouzení dopadu na základní práva proveďte před prvním zavedením systému. Za neprovedení hrozí pokuta až 7,5 mil. EUR nebo 1 % celosvětového obratu (tato sankce není stanovena Aktem o umělé inteligenci, nýbrž zatím pouze návrhem českého adaptačního zákona).

Povinnosti dovozců a distributorů

Dovozce

Před uvedením VRS na trh ověří posouzení shody, technickou dokumentaci, označení CE, EU prohlášení o shodě a jmenování zástupce; uvede své kontaktní údaje, zajistí skladování a přepravu a uchová dokumentaci 10 let.

Distributor

Před dodáním VRS ověří označení CE, EU prohlášení o shodě, návod k použití a splnění povinností poskytovatele i dovozce; nesouladný systém nedodá a zajistí nápravu, stažení z trhu či z oběhu.

LHŮTA Povinnosti zavádějících subjektů se uplatní od 2. 8. 2026. Novela AI Omnibus odkládá lhůtu u systémů podle přílohy III do 2. 12. 2027.

06 Obecné modely AI (GPAI)

Kapitola V upravuje obecné modely AI a rozlišuje modely **bez systémového rizika** a **se systémovým rizikem**. Poskytovatelé modelů se systémovým rizikem plní vedle obecných povinností i další, přísnější požadavky.

Termín, který nelze přehlédnout: povinnosti poskytovatelů obecných modelů AI platí už od 2. 8. 2025.

(A) Modely bez systémového rizika

POVINNOST	STRUČNÝ POPIS
Technická dokumentace modelu	Vypracovat a průběžně aktualizovat dokumentaci modelu a na žádost ji poskytnout úřadu pro AI a vnitrostátním orgánům.
Informace pro navazující poskytovatele	Zpřístupnit informace a dokumentaci poskytovatelům, kteří chtějí model začlenit do svých systémů AI.
Politika dodržování autorského práva	Zavést politiku pro soulad s autorským právem EU, včetně výjimky pro vytěžování textů a dat.
Shrnutí trénovacího obsahu	Vypracovat a zveřejnit dostatečně podrobné shrnutí trénovacího obsahu podle vzoru úřadu pro AI.
Součinnost	Spolupracovat s Evropskou komisí a vnitrostátními orgány a na žádost poskytnout dokumentaci a informace.
Přístup k modelu	Na odůvodněnou žádost poskytnout Komisi přístup k modelu (přes API či jinak), včetně zdrojového kódu.

U modelů pod svobodnou a otevřenou licencí (free and open-source) se část povinností k dokumentaci neuplatní; povinnosti k autorskému právu a shrnutí trénovacího obsahu zůstávají.

(B) Modely se systémovým rizikem

Model se systémovým rizikem má vysoké dopadové schopnosti, nebo ho za takový označí Evropská komise. Vedle obecných povinností musí jeho poskytovatel navíc:

POVINNOST	STRUČNÝ POPIS
Hodnocení modelu	Provádět hodnocení podle aktuálního stavu techniky, včetně kontradiktorního testování, a dokumentovat je.
Posuzování a zmírňování systémových rizik	Průběžně posuzovat a zmírňovat systémová rizika na úrovni EU, včetně jejich zdrojů.
Hlášení závažných incidentů	Sledovat, dokumentovat a bez zbytečného odkladu hlásit incidenty úřadu pro AI a vnitrostátním orgánům.
Kyberbezpečnost	Zajistit odpovídající kyberbezpečnost modelu i jeho fyzické infrastruktury.
Zplnomocněný zástupce	Poskytovatelé ze třetích zemí musí před uvedením na trh jmenovat zástupce v EU.

Sankce: za úmyslné či nedbalostní porušení může Evropská komise uložit pokutu až **15 mil. EUR** nebo **3 % celosvětového obratu** (podle toho, co je vyšší). Pokuty může ukládat od 2. 8. 2026.

07 Povinnosti transparentnosti

Kapitola IV cílí na situace, kdy člověk komunikuje se systémem AI nebo je vystaven obsahu, který AI vytvořila či upravila. Smyslem je, aby lidé věděli, s čím mají co do činění: chatboti, generátory syntetického obsahu, rozpoznávání emocí, deepfakes a vybrané AI texty o věcech veřejného zájmu.

PŘEHLED POVINNOSTÍ PODLE ROLE

KDO	SITUACE	POVINNOST
POSKYTOVATEL		
Poskytovatel	Systém komunikuje přímo s lidmi (chatbot, asistent)	Zajistit, aby osoby věděly, že komunikují s AI.
Poskytovatel	Systém generuje syntetický zvuk, obraz, video či text	Označit výstup strojově čitelně jako uměle vytvořený (u starších systémů do 2. 12. 2026).
ZAVÁDĚJÍCÍ SUBJEKT		
Zavádějící subjekt	Rozpoznávání emocí / biometrická kategorizace	Informovat vystavené osoby o provozu systému.
Zavádějící subjekt	Deepfake (obraz, zvuk, video)	Zveřejnit, že obsah byl uměle vytvořen či upraven.
Zavádějící subjekt	AI text o věcech veřejného zájmu	Zveřejnit umělý původ textu (neplatí po lidské redakční kontrole).

Informace podle čl. 50 musí být dotčeným osobám poskytnuty **jasně a rozlišitelně**, nejpozději při první interakci nebo vystavení systému, ne skryté v podmínkách či technických údajích.

Q Nejčastější otázky z praxe

OTÁZKA	ODPOVĚĎ
Musí být uživatel informován, že komunikuje s chatbotem?	Ano. Poskytovatel systému určeného k přímé interakci s lidmi musí zajistit, aby osoby věděly, že komunikují s AI.
Platí informační povinnost u chatbotů vždy?	Ne. Je-li zjevné, že jde o AI nástroj, výslovné upozornění není nutné.
Kdo odpovídá za označení syntetického obsahu?	Poskytovatel systému (včetně obecných systémů AI), který syntetický obsah vytváří. Výstupy musí být označeny strojově čitelně.
Stačí u AI obsahu metadata?	Klíčové je strojově čitelné označení výstupů. Nezaniká tím ale povinnost zavádějícího subjektu označit deepfake a vybrané texty.
Kdy informovat o rozpoznávání emocí či biometrické kategorizaci?	Zavádějící subjekt musí o provozu informovat vystavené osoby. Tím nejsou dotčeny povinnosti podle GDPR.
Musí být deepfake vždy označen?	Ano. Tvůrce musí zveřejnit, že obsah byl uměle vytvořen či změněn, aby jej příjemce nepovažoval za autentický.
Platí výjimka u uměleckého či satirického obsahu?	Povinnost je zmírněna, nezaniká: zveřejnění musí proběhnout vhodně, aniž naruší zobrazení nebo užití díla.

Nejčastější otázky · pokračování

OTÁZKA	ODPOVĚĎ
Musí být označen každý AI text?	Ne. Povinnost dopadá jen na text zveřejněný k informování veřejnosti o věcech veřejného zájmu.
Kdy AI text o veřejném zájmu označen být nemusí?	Pokud prošel lidskou redakční kontrolou a za zveřejnění nese redakční odpovědnost fyzická či právnická osoba.
Jak mají být informace podle čl. 50 poskytnuty?	Jasně a rozlišitelně, nejpozději při první interakci nebo vystavení, ne skryté v podmínkách či technických údajích.

MÁTE DOTAZ?

Zeptejte se přímo autora handbooku

jaroslav.mencik@ambit.law →

JUDr. Ing. Jaroslav Menčík LL.M, PhD.

partner advokátní kanceláře Ambit



08 Časová osa použitelnosti

AI Act se nerozbíhá najednou. Povinnosti nabíhají postupně. Vyplatí se vědět, co platí dnes a co teprve přijde.

1. 8. 2024 — Vstup Aktu o umělé inteligenci v platnost.

2. 2. 2025 — Použijí se ustanovení o zakázaných postupech a o zajištění gramotnosti v oblasti AI.

2. 8. 2025 — Začala se uplatňovat pravidla governance a povinnosti pro obecné modely AI.

2. 8. 2026 — Obecná použitelnost většiny ustanovení. AI Omnibus odkládá povinnosti VRS do 2. 12. 2027 (příloha III).

2. 8. 2027 — Prodloužené období pro VRS zabudované do regulovaných produktů. AI Omnibus odkládá lhůtu do 2. 8. 2028 (příloha I).

Compliance se staví postupně, stejně jako nabíhají povinnosti. Doporučený postup, který připraví na nejbližší termíny:

01

AI legal audit

Zmapování nástrojů a riziková klasifikace. Víte, co se vás týká a do kdy.

02

AI policy

Interní pravidla pro používání AI: jasná pravidla, role a odpovědnosti zaměstnanců před srpnem 2026.

03

Vysoce rizikové systémy

Posouzení shody a dokumentace s výhledem na lhůty 2027 a 2028.

09 Česká implementace

AI Act je přímo použitelné nařízení EU, ale členské státy musí doplnit institucionální, procesní a sankční rámec. V ČR je připravován adaptační zákon; návrh zákona o umělé inteligenci (a o změně zákona č. 87/2023 Sb.) předložený MPO je po meziresortním připomínkovém řízení. Pro podniky bude důležitý zejména pro určení dozorových orgánů, sandbox, posuzování shody, kontrolní postupy a sankce.

KDO BUDE HRÁT ROLI

Ministerstvo průmyslu a obchodu

Gestor implementace AI Actu v ČR.

Český telekomunikační úřad

Očekávaná významná role v dozoru nad trhem a koordinaci.

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

Zřizovatel regulačního sandboxu a oznamující orgán.

Česká agentura pro standardizaci

Očekávaná role při tvorbě a provozu regulatorního sandboxu.

10 GDPR a navazující regulace

AI Act nenahrazuje GDPR. Pokud systém AI pracuje s osobními údaji, musí organizace splnit oba režimy současně. V praxi se vyplatí nedělat oddělený „AI audit“ a „GDPR audit“, ale sjednotit je do jednoho procesu řízení datových a technologických rizik. Vedle AI Actu je třeba zohlednit i širší digitální a sektorovou regulaci. U konkrétního use casu může být rozhodující nikoli technologie, ale oblast, ve které je používána.

11 Compliance v šesti krocích

Cesta k souladu nemusí začínat rozsáhlým projektem. Osvědčil se nám rámec o šesti krocích, který umožní AI používat bezpečně a kontrolovaně, bez papírování pro papírování.

1	**Inventura AI nástrojů**	Zmapovat, kde všude se AI v organizaci reálně používá, včetně nástrojů, které si týmy zavedly samy.
2	**Klasifikace rizika**	Zařadit každé použití podle rizikovosti, od zakázaných praktik po systémy bez zvláštních povinností.
3	**Určení role**	U každého systému určit, zda jste poskytovatel, zavádějící subjekt, distributor, dovozce nebo výrobce.
4	**Kontrola smluv a dodavatelů**	Ošetřit dokumentaci, bezpečnost, data, auditní práva, incidenty a odpovědnost.
5	**Interní pravidla a školení**	Přijmout AI policy a proškolit lidi: schvalování nástrojů, zakázané vstupy, kontrola výstupů.
6	**Dokumentace a monitoring**	Compliance nasazením nekončí; modely se mění a s nimi i právní souvislosti.

ŠEST KROKŮ JE RÁMEC, NE HOTOVÁ CESTA

Ke každému kroku máme připravené nástroje: kontrolní seznamy, šablony AI policy, vzorová smluvní ujednání i rozhodovací schémata. Provedeme vás od první inventury až po compliance nastavené na míru vašemu byznysu.

12 Jak vám pomůžeme

Pomáháme klientům nastavit AI compliance prakticky, srozumitelně a s ohledem na jejich byznys, ne na úkor inovací, ale na jejich podporu.

AI legal audit

Zmapování nástrojů, riziková klasifikace, identifikace povinností.

AI policy a interní směrnice

Pravidla pro používání AI, schvalování use cases, odpovědnosti.

Smlouvy s dodavateli AI

Revize a příprava smluv, licencí, DPA, SLA, auditních práv a odpovědnosti.

GDPR a AI

DPIA, právní tituly, informační povinnosti, automatizované rozhodování a profilování.

AI v HR

Náborové algoritmy, hodnocení, monitoring, rovné zacházení a governance.

AI v marketingu a obsahu

AI obsah, deepfakes, označování, autorská práva, ochrana spotřebitele.

Vysoce rizikové systémy

Podpora u posouzení shody, dokumentace a komunikace s orgány dohledu.

Školení

Praktická školení managementu i zaměstnanců k regulaci a bezpečnému používání AI.

13 Závěr

Akt o umělé inteligenci není pouze technická regulace pro vývojáře. Je to nový právní rámec pro každou organizaci, která používá AI při rozhodování, komunikaci, práci s daty nebo poskytování služeb. Společnosti, které začnou včas, sníží regulatorní rizika a posílí důvěru zákazníků, zaměstnanců i partnerů.

AI compliance není překážka inovací. Správně nastavená pravidla umožňují využívat AI rychleji, bezpečněji a odpovědně.

O AMBIT PRÁVO PRO DIGITÁLNÍ DOBU

Advokátní kancelář Ambit se specializuje na komplexní právní služby s vysokou přidanou hodnotou. Mezi klienty Ambit patří startupy, scaleupy, velké korporace, investiční fondy (venture kapitálové fondy, private equity fondy, fondy fondů) a také banky. Je doporučovanou advokátní kanceláří pro venture kapitálové a private equity transakce, duševní vlastnictví, digitální ekonomiku a informační technologie.

Opakovaně ji v těchto oblastech oceňují prestižní žebříčky PitchBook, IFLR1000, Legal500 nebo Právnická firma roku. Ambit byl založen v roce 2017 advokátem Tomášem Ditrychem, od té doby má na kontě přes 300 uzavřených M&A transakcí v technologickém segmentu.

OCENĚNÍ

IFLR1000
Notable Service Provider
M&A (2023, 2024, 2025)
Banking & Finance (2024, 2025)

Czech Law Firm of The Year 2025
Recommended Law Firm
M&A (2025)
Capital Markets (2025)
IT Law (2023, 2024, 2025)

The LEGAL 500
Firm To Watch
Commercial, Corporate and M&A
(2024, 2025)

PitchBook a Morningstar company
Most Active Law Firm
VC Deals in CEE
(2023, 2024, 2025)

KONTAKT

Ambit advokáti, s.r.o.
Na Příkopě 1047/17
110 00 Praha 1, Staré Město
Česká republika

Jaroslav Menčík, partner
E: jaroslav.mencik@ambit.law
W: www.ambit.law

Where Ambition Meets Execution

© 2026 Ambit · Všechna práva vyhrazena.

Pro více informací o tomto e-booku nebo pokud si přejete být zařazeni do e-mailového seznamu pro odběr (bez poplatku), kontaktujte prosím info@ambit.law.

Tento materiál má informativní charakter a nenahrazuje individuální právní poradenství. Nepředstavuje právní radu a není zamýšlen k vytvoření vztahu advokát-klient. Stav legislativy a termíny ověřujte podle aktuálního znění.

Žádná část tohoto e-booku nesmí být reprodukována v jakékoli formě bez výslovného písemného svolení společnosti Ambit.

www.ambit.law