Študijná Príručka: Európska Legislatíva o Umelej Inteligencii

Kvíz (krátke odpovede)

1. Aké sú hlavné kategórie rizika, podľa ktorých AI Act klasifikuje AI systémy?
2. Vymenujte aspoň tri špecifické požiadavky, ktoré AI Act stanovuje pre vysokorizikové AI systémy.
3. Aký je vzťah medzi posúdením vplyvu na ochranu údajov (DPIA) a posúdením vplyvu na základné práva (FRIA) v kontexte AI Actu?
4. Aké hlavné povinnosti ukladá smernica NIS2 prevádzkovateľom základnej služby (PZS) v oblasti kybernetickej bezpečnosti, a ako to súvisí s AI systémami?
5. Čo by mali obsahovať zmluvy s IKT poskytovateľmi v kontexte AI systémov, najmä s ohľadom na kybernetickú bezpečnosť a ochranu údajov?
6. Aká významná zmena v oblasti zodpovednosti za škodu spôsobenú AI nadobudne účinnosť 9. decembra 2026?
7. Aké špecifické aspekty je potrebné zohľadniť pri používaní AI systémov v náborovom procese z hľadiska AI Actu?
8. Aké sú niektoré z hlavných regulačných výziev spojených s veľkými jazykovými modelmi (LLM)?
9. Aké nariadenie reguluje kybernetickú bezpečnosť produktov s digitálnymi prvkami (vrátane AI) pri ich uvedení na trh EÚ pred nadobudnutím účinnosti AI Aktu?
10. Aký je rozdiel medzi rolou poskytovateľa a nasadzujúceho subjektu AI systému z pohľadu povinností vyplývajúcich z AI Aktu?

Kľúč odpovedí ku kvízu

1. Hlavné kategórie rizika sú zakázané praktiky, vysokorizikové, obmedzené a minimálne riziko. Táto klasifikácia je založená na potenciálnom ohrození zdravia, bezpečnosti a základných práv občanov EÚ.
2. Medzi špecifické požiadavky pre vysokorizikové AI systémy patria riadenie rizík, kvalita dát, zohľadnenie zaujatosti, technická dokumentácia vrátane opatrení kybernetickej bezpečnosti, logovanie, transparentnosť, ľudský dohľad a samotná kybernetická bezpečnosť.
3. FRIA nadväzuje na DPIA a dopĺňa ho, pričom sa zameriava primárne na potenciálne negatívne dopady na dotknuté osoby a zásahy do ich základných práv, a to aj v prípadoch, keď nedôjde k narušeniu bezpečnosti osobných údajov.
4. Smernica NIS2 ukladá PZS povinnosť vykonať analýzu rizík a na jej základe implementovať všeobecné bezpečnostné opatrenia. Táto povinnosť sa vzťahuje aj na riadenie rizík spojených s dodávateľmi AI systémov a zabezpečenie ich kybernetickej bezpečnosti.
5. Zmluvy by mali jasne definovať zodpovednosť za bezpečnosť a ochranu údajov, povinnosti týkajúce sa auditov, testovaní a certifikácií, postupy pri incidentoch a ich oznamovaní, a mechanizmy pre ochranu pred technologickými poruchami a obnovu systémov. Pre finančný sektor DORA stanovuje ešte špecifickejšie požiadavky.

6. Od 9. decembra 2026 sa softvér a AI budú považovať za "výrobok" v zmysle smernice o zodpovednosti za chybné výrobky, čo povedie k sprísneniu podmienok náhrady škody a presunu dôkazného bremena v technicky komplexných prípadoch na výrobcu.
7. Pri náborovom procese je potrebné skontrolovať klasifikáciu AI systému podľa rizika, jasne rozlišovať povinnosti poskytovateľa a nasadzujúceho subjektu, zabezpečiť AI gramotnosť zamestnancov a vyžadovať od dodávateľov komplexnú dokumentáciu preukazujúcu súlad s AI Actom a opatrenia na zmiernenie rizík.
8. Hlavné výzvy LLM zahŕňajú ich "čiernu skrinku" fungovanie, potenciálne slabé stránky ako halucinácie a zaujatosti, a otázky týkajúce sa zodpovednosti za generovaný obsah, ochrany súkromia, duševného vlastníctva a kybernetickej bezpečnosti.
9. Nariadenie CRA (Cyber Resilience Act) reguluje kybernetickú bezpečnosť produktov s digitálnymi prvkami (vrátane AI) pri ich uvedení na trh EÚ pred nadobudnutím účinnosti AI Aktu, pričom jeho aplikácia nezávisí od klasifikácie AI systému podľa AI Aktu.
10. Poskytovateľ (vývojár) AI systému má primárnu zodpovednosť za zabezpečenie súladu s AI Actom a inými relevantnými predpismi EÚ, zatiaľ čo nasadzujúci subjekt (používateľ) má povinnosti najmä v súvislosti s používaním vysokorizikových systémov v súlade s ich určeným účelom a návodmi na použitie.

Návrhy esejových otázok

1. Analyzujte kľúčové prepojenia medzi AI Actom a existujúcimi európskymi právnymi predpismi, ako sú GDPR, smernica NIS2 a nariadenie DORA. Ako tieto prepojenia prispievajú k holistickému prístupu k regulácii umelej inteligencie?
2. Diskutujte o koncepte klasifikácie AI systémov podľa rizika v AI Acte. Aké sú výhody a potenciálne nevýhody tohto prístupu pre inovácie a ochranu základných práv?
3. Preskúmajte povinnosti poskytovateľov a nasadzujúcich subjektov vysokorizikových AI systémov podľa AI Actu. Aké sú hlavné výzvy pri zabezpečovaní súladu s týmito povinnosťami v praxi?
4. Zhodnoťte dopad novej úpravy zodpovednosti za škodu spôsobenú AI na výrobcov softvéru a AI a na ochranu spotrebiteľov v Európskej únii. Aké sú potenciálne dôsledky pre vývoj a používanie AI technológií?
5. Na základe poskytnutých zdrojov analyzujte špecifické regulačné výzvy a odporúčania týkajúce sa používania umelej inteligencie v oblasti náboru zamestnancov a vo finančnom sektore. Ako AI Act a súvisiace právne predpisy ovplyvňujú tieto odvetvia?

Glosár kľúčových pojmov

- **AI Act (Akt o umelej inteligencii):** Nová európska legislatíva, ktorej cieľom je regulovať vývoj, uvádzanie na trh a používanie systémov umelej inteligencie v Európskej únii.
- **Vysokorizikový AI systém:** AI systém, ktorý bol identifikovaný ako potenciálne predstavujúci významné riziko pre zdravie, bezpečnosť alebo základné práva osôb. Podlieha prísnym požiadavkám AI Aktu.

- **Poskytovateľ (AI systému):** Fyzická alebo právnická osoba, ktorá vyvíja AI systém alebo necháva AI systém vyvinúť a uvádza ho na trh alebo do prevádzky pod svojím vlastným menom alebo ochrannou známkou, či už za odplatu alebo bezplatne.
- **Nasadzujúci subjekt (používateľ AI systému):** Fyzická alebo právnická osoba, ktorá používa AI systém pod svojím vedením, s výnimkou prípadov, keď sa AI systém používa v rámci osobnej, nedotknutej profesionálnej činnosti.
- **GDPR (General Data Protection Regulation):** Všeobecné nariadenie o ochrane údajov, právny rámec EÚ upravujúci spracúvanie osobných údajov fyzických osôb.
- **DPIA (Data Protection Impact Assessment):** Posúdenie vplyvu na ochranu údajov, proces na identifikáciu a posúdenie rizík pre ochranu osobných údajov spojených so spracovateľskými činnosťami.
- **FRIA (Fundamental Rights Impact Assessment):** Posúdenie vplyvu na základné práva, proces na posúdenie potenciálneho negatívneho vplyvu AI systému na základné práva dotknutých osôb.
- **NIS2 (Smernica o sieťovej a informačnej bezpečnosti):** Smernica EÚ zameraná na zvýšenie úrovne kybernetickej bezpečnosti v celej Únii, týkajúca sa prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb.
- **Zákon o kybernetickej bezpečnosti (ZKB):** Slovenská legislatíva implementujúca smernicu NIS2, upravujúca povinnosti v oblasti kybernetickej bezpečnosti pre určené subjekty.
- **DORA (Digital Operational Resilience Act):** Nariadenie EÚ o digitálnej prevádzkovej odolnosti finančného sektora, stanovujúce jednotné pravidlá pre riadenie rizika IKT.
- **Kybernetická bezpečnosť:** Schopnosť sietí a informačných systémov odolávať udalostiam, ktoré by mohli ohroziť dostupnosť, integritu, dôvernosť a autenticitu uchovávaných, prenášaných alebo spracúvaných údajov a súvisiacich služieb.
- **LLM (Large Language Model):** Veľký jazykový model, typ modelu umelej inteligencie, ktorý je trénovaný na rozsiahlych textových dátach a je schopný generovať text podobný ľudskému.
- **CRA (Cyber Resilience Act):** Nariadenie o kybernetickej odolnosti, ktoré stanovuje základné požiadavky na kybernetickú bezpečnosť produktov s digitálnymi prvkami.
- **Poskytovateľ GPAI (všeobecných modelov AI):** Poskytovateľ AI modelu, ktorý je trénovaný na rozsiahlych dátach, má všeobecné schopnosti a môže byť použitý pre rôzne úlohy.
- **Zakázané praktiky (v AI):** Praktiky používania AI, ktoré sú považované za škodlivé a sú AI Actom zakázané (napr. niektoré formy biometrického rozpoznávania na diaľku v reálnom čase).