Podrobná súhrnná správa k európskej legislatíve o umelej inteligencii

Táto správa sumarizuje kľúčové témy, najdôležitejšie myšlienky a fakty vyplývajúce z poskytnutých zdrojov týkajúcich sa novej európskej legislatívy o umelej inteligencii (AI Act) a jej prepojenia s existujúcimi právnymi predpismi, ako sú GDPR, smernica NIS2, Zákon o kybernetickej bezpečnosti a nariadenie DORA. Dôraz sa kladie na klasifikáciu AI systémov podľa rizika, povinnosti pre poskytovateľov a používateľov, otázky zodpovednosti, bezpečnosti (vrátane kybernetickej bezpečnosti), zmluvné aspekty a špecifické aplikácie AI v rôznych odvetviach (napr. nábor zamestnancov a finančný sektor).

1. AI Act a jeho základné princípy:

- AI systémy budú klasifikované podľa úrovne rizika, ktoré predstavujú pre zdravie, bezpečnosť a základné práva občanov EÚ. Kategórie rizika zahŕňajú zakázané praktiky, vysokorizikové, obmedzené a minimálne riziko.
- Pre **vysokorizikové AI systémy** stanovuje AI Act špecifické požiadavky v článkoch 8 až 15, týkajúce sa:
- **Riadenia rizík:** Poskytovatelia musia zaviesť a udržiavať systém riadenia rizík ("*vysokorizikové systémy AI musia spĺňať špecifické požiadavky stanovené v článkoch 8 až 15 AI Aktu, týkajúce sa riadenia rizík...*").
- **Kvality dát:** Dátové sady použité pre vývoj vysokorizikových AI systémov musia byť relevantné, reprezentatívne a bez chýb ("*kvality dát*").
- **Zohľadnenia zaujatosti:** Je potrebné prijímať opatrenia na identifikáciu a zmiernenie potenciálnej zaujatosti v AI systémoch ("*zohľadnenia zaujatosti*").
- **Technickej dokumentácie:** Poskytovatelia musia pripraviť a uchovávať podrobnú technickú dokumentáciu ("*technickej dokumentácie*"). Táto dokumentácia musí obsahovať aj opatrenia v oblasti kybernetickej bezpečnosti ("*Technická dokumentácia k vysokorizikovým AI systémom musí obsahovať aj opatrenia v oblasti kybernetickej bezpečnosti*").
- **Logovania:** Vysokorizikové AI systémy musia byť schopné automaticky zaznamenávať udalosti relevantné pre monitorovanie ich fungovania a posúdenie rizík ("*logovania*").
- **Transparentnosti:** Používatelia musia byť informovaní o tom, že interagujú s AI systémom, pokiaľ to nie je zjavné a primerané v danom kontexte ("*transparentnosti*").
- **Ľudského dohľadu:** Vysokorizikové AI systémy musia byť navrhnuté tak, aby umožňovali efektívny ľudský dohľad ("*ľudského dohľadu*").
- **Kybernetickej bezpečnosti:** Vysokorizikové AI systémy musia byť odolné voči kybernetickým útokom a manipulácii ("*kybernetickej bezpečnosti*"). Musia byť navrhnuté tak, aby dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti počas celého ich životného cyklu ("*Vysokorizikové AI systémy musia byť navrhnuté tak, aby dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti počas celého ich životného cyklu... To zahŕňa aj odolnosť voči poruchám a kybernetickým útokom (napr. otráveniu dát)*").
- **Poskytovatelia** vysokorizikových AI systémov nesú primárnu zodpovednosť za zabezpečenie súladu s AI Actom a inými relevantnými právnymi predpismi EÚ ("*Poskytovatelia musia zabezpečiť súlad AI systémov s ďalšími relevantnými právnymi predpismi EÚ*").

- **Nasadzujúce subjekty (používatelia)** majú tiež povinnosti, najmä v súvislosti s používaním vysokorizikových systémov v súlade s ich určeným účelom a návodmi na použitie.

2. Prepojenie s GDPR a FRIA:

- Pripravovaný AI Act úzko súvisí s GDPR, najmä v oblasti spracúvania osobných údajov AI systémami. Pri spracúvaní osobných údajov je potrebné vykonať **posúdenie vplyvu na ochranu údajov (DPIA)** ("*V prípade spracúvania osobných údajov vykonajte posúdenie vplyvu na ochranu údajov (DPIA)*").

- AI Act zavádza koncept **posúdenia vplyvu na základné práva (FRIA)**, ktorý nadväzuje na DPIA a dopĺňa ho ("*Uvedomte si úzke prepojenie medzi DPIA a posúdením vplyvu na základné práva (FRIA) podľa pripravovaného AI Aktu... FRIA na DPIA nadväzuje a dopĺňa ho*"). FRIA sa zameriava primárne na potenciálne negatívne dopady na dotknuté osoby a zásahy do ich práv, a to aj v prípadoch, keď nedôjde k narušeniu bezpečnosti osobných údajov ("*Pri vypracovaní DPIA a FRIA zamerajte sa primárne na potenciálne negatívne dopady na dotknuté osoby, a to aj v prípadoch, keď nedôjde k narušeniu bezpečnosti... Identifikujte možné životné situácie a zásahy do ich práv*").

- DPIA a FRIA sú nástroje ochrany osobných údajov, zamerané na práva dotknutých osôb, a presahujú rámec základnej bezpečnosti údajov ("*DPIA a FRIA sú nástroje ochrany osobných údajov, zamerané na práva dotknutých osôb, a idú nad rámec základnej bezpečnosti*"). Je dôležité rozlišovať medzi "ochranou osobných údajov" a "bezpečnosťou údajov" ("*Rozlišujte medzi pojmami 'ochrana osobných údajov' (data protection) a 'bezpečnosť údajov' (data security)*").

- Pri implementácii FRIA sa odporúča postupovať v troch fázach: plánovanie a stanovenie rozsahu, zber údajov a analýza rizík, a riadenie rizík ("*Pri implementácii FRIA sa odporúča postupovať v troch fázach: plánovanie a stanovenie rozsahu, zber údajov a analýza rizík, a riadenie rizík*"). Kľúčové je zohľadniť perspektívu dotknutých osôb ("*V rámci FRIA je kľúčové zohľadniť perspektívu dotknutých osôb*").

3. Prepojenie so smernicou NIS2 a Zákonom o kybernetickej bezpečnosti:

- Kybernetická bezpečnosť vysokorizikových AI systémov je kľúčovou oblasťou regulácie a prelína sa s požiadavkami AI Aktu, smernice NIS2 a Zákona o kybernetickej bezpečnosti (ZKB) ("*Kybernetická bezpečnosť vysokorizikových AI systémov je regulovaná prostredníctvom AI Aktu, ZKB/NIS2, GDPR a DORA*").

- Prevádzkovatelia základnej služby (PZS) sú povinní vykonávať analýzu rizík a na jej základe implementovať všeobecné bezpečnostné opatrenia ("*Prevádzkovatelia základnej služby (PZS) sú povinní vykonať analýzu rizík a na jej základe implementovať všeobecné bezpečnostné opatrenia... Analýza rizík je základným pilierom zákona o kybernetickej bezpečnosti*"). Táto povinnosť sa vzťahuje aj na uzatváranie zmlúv s IKT poskytovateľmi a dodávateľmi AI systémov ("*Analýza rizík sa vyžaduje aj pri uzatváraní zmlúv s IKT poskytovateľmi... Pri výbere dodávateľov AI systémov venujte pozornosť dokumentácii (vrátane klasifikácie podľa AI Aktu)...*").

- Zmluvy s IKT poskytovateľmi musia 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 ("*Zmluvy s IKT poskytovateľmi 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").

- AI Act vyžaduje, aby vysokorizikové AI systémy boli odolné voči kybernetickým útokom ("*AI Akt vyžaduje... osobitné požiadavky na kybernetickú bezpečnosť, ako je odolnosť voči poruchám a ochrana pred útokmi (otrávenie dát, oklamanie modelov)*"). Certifikácia kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 (Cybersecurity Act) môže prispieť k preukázaniu súladu s požiadavkami na kybernetickú bezpečnosť podľa AI Aktu ("*Certifikácia kybernetickej bezpečnosti podľa nariadenia (EÚ) 2019/881 môže prispieť k preukázaniu súladu s požiadavkami na kybernetickú bezpečnosť podľa AI Aktu*").
- Do nadobudnutia účinnosti AI Aktu, nariadenie CRA (Cyber Resilience Act) reguluje kybernetickú bezpečnosť produktov s digitálnymi prvkami (vrátane AI) pri ich uvedení na trh EÚ ("*Do nadobudnutia účinnosti AI Aktu, nariadenie CRA (Cyber Resilience Act) reguluje kybernetickú bezpečnosť produktov s digitálnymi prvkami (vrátane AI) pri ich uvedení na trh EÚ*").

4. Zmluvné aspekty AI systémov:

- Pri vývoji a implementácii AI systémov je kľúčové dôkladne riešiť zmluvné aspekty s dodávateľmi ("*Pri výbere dodávateľov AI systémov venujte pozornosť... zmluvným podmienkam...*").
- Zmluvy by mali jasne definovať povolené spôsoby použitia AI systémov a obmedziť zodpovednosť dodávateľa ("*Jasne definujte povolené spôsoby použitia AI systémov a obmedzte zodpovednosť dodávateľa v zmluvách... Stanovte podmienky používania a zodpovednosť za výsledky a prípadné porušenia práv*").
- Je potrebné riešiť otázky týkajúce sa tréningových dát (ich zdroj, typ, ochrana duševného vlastníctva), duševného vlastníctva samotného modelu AI a jeho výstupov ("*Pri vývoji AI systémov dôkladne riešte otázky týkajúce sa tréningových dát: ich zdroj, typ (osobné vs. neosobné), ochrana duševného vlastníctva a súvisiace právne aspekty (web scraping)... Riešte otázky duševného vlastníctva týkajúce sa tréningových dát, samotného modelu AI a jeho výstupov*").
- Zmluvy by mali obsahovať ustanovenia o robustnosti a bezpečnosti AI systémov a zohľadňovať potenciálne hrozby a útoky ("*Dbajte na robustnosť a bezpečnosť AI systémov a zohľadnite potenciálne hrozby a útoky*").
- Pre finančný sektor, nariadenie DORA stanovuje špecifické požiadavky na obsah zmlúv s externými poskytovateľmi IKT služieb, vrátane podrobného opisu služieb, informácií o lokalite spracúvania a uchovávania údajov, ustanovení o obnove a návrate údajov, SLA, postupov pri incidentoch, pravidiel spolupráce s orgánmi a podmienok ukončenia zmluvy ("*Pre finančný sektor, podľa nariadenia DORA, by zmluvy s externými poskytovateľmi IKT služieb mali obsahovať podrobný opis služieb, informácie o lokalite spracúvania a uchovávania údajov, ustanovenia o obnove a návrate údajov, SLA, postupy pri incidentoch, pravidlá spolupráce s orgánmi a podmienky ukončenia zmluvy*").

5. Zodpovednosť za škodu spôsobenú AI:

- S účinnosťou 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 ("*S účinnosťou 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*").
- Výrobcovia softvéru a AI (vrátane vývojárov aplikácií, SaaS a AI modelov) budú niesť zodpovednosť za škodu spôsobenú chybnými výrobkami ("*Výrobcovia softvéru a AI (vrátane vývojárov aplikácií, SaaS a AI modelov) budú niesť zodpovednosť za škodu spôsobenú chybnými výrobkami*"). Zodpovednosť sa bude vzťahovať aj na chyby spôsobené aktualizáciami, učením AI, IT zraniteľnosťami a poškodením dát ("*Zodpovednosť sa bude vzťahovať aj na chyby spôsobené aktualizáciami softvéru a AI, chybami vyplývajúcimi z učenia AI, IT zraniteľnosťami a zničeniu alebo poškodeniu dát*").
- V prípade sporu bude dôkazné bremeno v technicky komplexných prípadoch na strane výrobcu ("*V prípade sporu bude dôkazné bremeno v technicky komplexných prípadoch na strane výrobcu*").
- Okrem zodpovednosti podľa smernice o chybách výrobkov existuje aj zodpovednosť podľa Občianskeho zákonníka. Za konanie AI zodpovedá subjekt, ktorý ju vytvoril, nasadil alebo používa ("*Za konanie AI zodpovedá subjekt, ktorý ju vytvoril, nasadil alebo používa*").

6. AI v špecifických odvetviach (nábor):

- Pri používaní AI systémov v náborovom procese je potrebné skontrolovať ich klasifikáciu podľa AI Aktu, ktorá závisí od posúdenia rizika pre zdravie, bezpečnosť a základné práva ("*Pri používaní AI systémov v náborovom procese skontrolujte ich klasifikáciu podľa AI Aktu, ktorá závisí od posúdenia rizika pre zdravie, bezpečnosť a základné práva (vrátane práva na prácu, rovnaké zaobchádzanie a súkromie)*").
- Je dôležité rozlišovať medzi rolou nasadzujúceho subjektu (používateľa) a poskytovateľa (vývojára) AI systému, pretože každá z týchto rolí má odlišné povinnosti podľa AI Aktu ("*Jasne rozlišujte medzi rolou nasadzujúceho subjektu (používateľa) a poskytovateľa (vývojára) AI systému, pretože každá z týchto rolí má odlišné povinnosti podľa AI Aktu*").
- Je potrebné zabezpečiť dostatočnú úroveň AI gramotnosti pre zamestnancov pracujúcich s AI v náborovom procese ("*Zabezpečte dostatočnú úroveň AI gramotnosti pre všetkých zamestnancov, ktorí pracujú s AI systémami v náborovom procese*").
- Pri výbere dodávateľa AI pre nábor je potrebné vyžadovať komplexnú dokumentáciu preukazujúcu súlad s AI Aktom, opatrenia na zmiernenie rizík (vrátane zaujatosti a ľudského dohľadu), princípy fungovania algoritmu a možnosti výkonu práv dotknutých osôb ("*Pri výbere dodávateľa AI systémov pre nábor vyžadujte komplexnú dokumentáciu, ktorá preukazuje súlad s AI Aktom, opisuje prijaté opatrenia na zmiernenie rizík (vrátane zaujatosti a ľudského dohľadu), princípy fungovania algoritmu a možnosti výkonu práv dotknutých osôb*").

7. Výzvy a odporúčania:

- Veľké jazykové modely (LLM) predstavujú špecifické regulačné výzvy kvôli ich "čiernej skrinke" fungovaniu a potenciálnym slabým stránkam, ako sú halucinácie a zaujatosti ("*Uvedomte si, že veľké jazykové modely (LLM) fungujú na princípe predpovedania*

nasledujúceho slova a ich vnútorné fungovanie je často 'čiernou skrinkou'... Buďte si vedomí slabých stránok LLM, ako sú falošné tvrdenia (halucinácie), zaujatosti, nelogické výstupy a chyby vo výpočtoch").

- Je potrebné zabezpečiť dostatočnú úroveň gramotnosti v oblasti AI a kybernetickej bezpečnosti v rámci organizácie ("*Zabezpečte dostatočnú úroveň gramotnosti v oblasti AI v rámci organizácie... Bezpečnostné opatrenia musia zahŕňať vzdelávanie a budovanie bezpečnostného povedomia v oblasti kybernetickej bezpečnosti*").
- Organizácie by mali pravidelne monitorovať legislatívny proces, revidovať zmluvnú a bezpečnostnú dokumentáciu a pripraviť sa na implementáciu požiadaviek AI Aktu ("*Odporúča sa pravidelne monitorovať legislatívny proces, revidovať zmluvnú a bezpečnostnú dokumentáciu a zabezpečiť asistenciu pri kontrolách a plnení notifikačných povinností*").
- Pri výbere dodávateľov AI systémov je nevyhnutné venovať pozornosť nielen technickým aspektom, ale aj právnym a etickým aspektom, vrátane transparentnosti a súladu s novou legislatívou.

Táto správa poskytuje prehľad o komplexnej problematike regulácie umelej inteligencie v Európe. Je dôležité, aby dotknuté subjekty pozorne sledovali vývoj implementácie AI Aktu a prispôsobili svoje postupy a zmluvné vzťahy novým požiadavkám.