Tieto zdroje poskytujú prehľad o nových európskych právnych predpisoch týkajúcich sa umelej inteligencie, známych ako AI Act, a ich prepojení s existujúcimi zákonmi o kybernetickej bezpečnosti, ochrane osobných údajov (GDPR) a digitálnej prevádzkovej odolnosti finančného sektora (DORA). Dokumenty objasňujú klasifikáciu AI systémov podľa rizika, povinnosti pre poskytovateľov a používateľov vysokorizikových systémov, ako aj otázky zodpovednosti za škodu spôsobenú AI a bezpečnosti týchto systémov v kontexte kybernetických hrozieb. Zdroje tiež načrtávajú zmluvné aspekty pri využívaní IKT služieb a špecifiká týkajúce sa umelej inteligencie v rôznych odvetviach, vrátane náboru zamestnancov a finančného sektora.

Zhrnutie PDF podkladov do odporúčaní:

berthoty425.pdf - Ako neopakovať chyby z DPIA pri vypracovaní FRIA:

• **Rozlišujte medzi pojmami "ochrana osobných údajov" (data protection) a "bezpečnosť údajov" (data security)**1 . DPIA a FRIA sú nástroje ochrany osobných údajov, zamerané na práva dotknutých osôb, a idú nad rámec základnej bezpečnosti2 ....

• Pri vypracovaní DPIA a FRIA **zamerajte sa primárne na potenciálne negatívne dopady na dotknuté osoby**, a to aj v prípadoch, keď nedôjde k narušeniu bezpečnosti4 .... Identifikujte možné životné situácie a zásahy do ich práv5 ....

• **DPIA je nástroj riadenia rizík pre práva dotknutých osôb**, ktorý zohľadňuje ich pohľad, na rozdiel od riadenia rizík informačnej bezpečnosti, ktoré je zamerané na organizáciu2 .

• **Vyhnite sa chybnému prístupu, kde DPIA slúži len ako ďalšia analýza rizík informačnej bezpečnosti**3 . Skutočné DPIA by mali abstrahovať od základnej úrovne bezpečnosti a hodnotiť dopady na konkrétne práva a slobody FO3 ....

• Uvedomte si **úzke prepojenie medzi DPIA a posúdením vplyvu na základné práva (FRIA)** podľa pripravovaného AI Aktu7 .... FRIA na DPIA nadväzuje a dopĺňa ho3 ....

• Pri implementácii FRIA sa odporúča **postupovať v troch fázach**: plánovanie a stanovenie rozsahu, zber údajov a analýza rizík, a riadenie rizík9 .

• V rámci FRIA je kľúčové **zohľadniť perspektívu dotknutých osôb**10 .

• Pre FRIA **využívajte dostupné metodiky a usmernenia**, ako napríklad katalánsky vzor11 .

• **Dozorné orgány pre ochranu osobných údajov (DPA) môžu zohrávať aktívnu úlohu pri presadzovaní povinností FRIA** pri zavádzaní AI systémov, a to aj prostredníctvom ustanovení GDPR o posúdení vplyvu11 .

chlipala425.pdf - Smernica NIS2 a Zákon o kybernetickej bezpečnosti:

•**Prevádzkovatelia základnej služby (PZS)** sú povinní **vykonať analýzu rizík** a na jej základe implementovať **všeobecné bezpečnostné opatrenia**12 . Analýza rizík je základným pilierom zákona o kybernetickej bezpečnosti12 .

• **PZS sú povinní uzatvárať zmluvy s tretími stranami**, ak prostredníctvom nich vykonávajú činnosti priamo súvisiace s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov13 . Tieto zmluvy musia zabezpečiť plnenie bezpečnostných opatrení a notifikačných povinností13 .

• **Analýza rizík sa vyžaduje aj pri uzatváraní zmlúv s IKT poskytovateľmi**12 ....

• 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**15 .

• 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 zmluvy16 ....

• **Zabezpečte dostatočnú úroveň gramotnosti v oblasti AI** v rámci organizácie18 ....

• Pri výbere dodávateľov AI systémov venujte pozornosť **dokumentácii (vrátane klasifikácie podľa AI Aktu), spracúvaniu dát, zmluvným podmienkam, právnemu základu, DPIA, transparentnosti a gramotnosti**18 ....

• Bezpečnostné opatrenia musia zahŕňať **vzdelávanie a budovanie bezpečnostného povedomia** v oblasti kybernetickej bezpečnosti21 ....

kisely425.pdf - Contracting for Artificial Intelligence Systems:

• 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)23 ....

• Uvedomte si, že **testovanie AI systémov sa líši od testovania tradičného softvéru**28 . Akceptačné kritériá môžu byť komplexné a výstupy AI môžu byť variabilné28 .

• Jasne **definujte povolené spôsoby použitia AI systémov** a obmedzte zodpovednosť dodávateľa v zmluvách24 .... Stanovte podmienky používania a zodpovednosť za výsledky a prípadné porušenia práv24 .

• Riešte **otázky duševného vlastníctva** týkajúce sa tréningových dát, samotného modelu AI a jeho výstupov24 .

• Zabezpečte **ochranu súkromia** pri spracúvaní údajov AI systémami, vrátane transparentnosti, anonymizácie, retencie a dodržiavania práv dotknutých osôb25 . V prípade spracúvania osobných údajov **vykonajte posúdenie vplyvu na ochranu údajov (DPIA)**25 .

• Dbajte na **robustnosť a bezpečnosť AI systémov** a zohľadnite potenciálne hrozby a útoky25 .

• V zmluvách s dodávateľmi AI systémov **zahrňte povinnosti pre zákazníka/užívateľa** vyplývajúce zo špecifického zamerania modelu alebo obmedzení pre vysoko rizikové systémy29 . Zabezpečte **vyškolenie užívateľov**29 .

meszarosova425.pdf - RECRUITMENT VO SVETLE AI ACTU:

• 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)31 ....

• Jasne **rozlišujte medzi rolou nasadzujúceho subjektu (používateľa) a poskytovateľa (vývojára) AI systému**, pretože každá z týchto rolí má odlišné povinnosti podľa AI Aktu33 .... Zmena značky alebo podstatná zmena AI systému môže zmeniť postavenie na poskytovateľa33 ....

• **Zabezpečte dostatočnú úroveň AI gramotnosti** pre všetkých zamestnancov, ktorí pracujú s AI systémami v náborovom procese18 ....

• 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 osôb18 .... Overte **právny základ pre spracúvanie osobných údajov** a existenciu **DPIA**20 .

• Porovnajte požiadavky **GDPR a AI Aktu** v kontexte automatizovaného individuálneho rozhodovania a transparentnosti v náborovom procese20 ....

• Ak ste **vývojárom AI systémov pre nábor**, zabezpečte **AI gramotnosť**, poskytnite **jasné podmienky používania (návod)**, implementujte **monitorovanie a kontrolu** systému, zabezpečte **ľudský dohľad** a **preskúmateľnosť rozhodnutí**19 ....

• Zvážte **právne aspekty web scrapingu**, ak sa používa na získavanie dát pre AI systémy v náborovom procese26 ....

motuzova425.pdf - ZODPOVEDNOSŤ ZA VADY SOFTVÉRU AKO VÝROBKU:

• 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 škody36 .

• **Výrobcovia softvéru a AI (vrátane vývojárov aplikácií, SaaS a AI modelov)** budú niesť zodpovednosť za škodu spôsobenú chybnými výrobkami37 . Za výrobcu sa považuje aj subjekt, ktorý sa tak prezentuje (napr. uvedením vlastného mena)37 .

• Zodpovednosť sa bude vzťahovať aj na **chyby spôsobené aktualizáciami softvéru a AI**, chybami vyplývajúcimi z **učenia AI**, **IT zraniteľnosťami** a **zničeniu alebo poškodeniu dát**38 .

• V prípade sporu bude **dôkazné bremeno** v technicky komplexných prípadoch **na strane výrobcu**39 .

• Existujú určité **výnimky zo zodpovednosti**, ako napríklad "state of the art" (ktorého aplikácia na AI je otázna), spoluzodpovednosť spotrebiteľa a open source softvér na nekomerčné účely39 .

• **Online platformy** (ako app stores) budú niesť **zvýšenú zodpovednosť**39 .

• Výrobcovia by mali klásť **zvýšený dôraz na IT a kybernetickú bezpečnosť** a sledovanie dodávateľského reťazca39 . Odporúča sa **transparentná a etická AI**39 .

palasta425.pdf - AI a regulačné “problémy”:

• Uvedomte si, že **veľké jazykové modely (LLM)** fungujú na princípe predpovedania nasledujúceho slova a ich vnútorné fungovanie je často **"čiernou skrinkou"**40 ....

• Buďte si vedomí **slabých stránok LLM**, ako sú **falošné tvrdenia (halucinácie), zaujatosti, nelogické výstupy a chyby vo výpočtoch**41 .

• Regulačné orgány sa čoraz viac zameriavajú na **zákonnosť, presnosť a nepredvídateľnosť výstupov AI**43 .

• Zvážte **otázky zodpovednosti** za obsah generovaný AI, **ochrany súkromia, duševného vlastníctva a kybernetickej bezpečnosti** v kontexte používania AI43 ....

• Oboznámte sa s princípmi **zodpovednosti za škodu podľa Občianskeho zákonníka** a ako sa aplikujú na prípady, keď škodu spôsobí AI42 .... Za konanie AI zodpovedá subjekt, ktorý ju vytvoril, nasadil alebo používa47 .

• Rozlišujte medzi **subjektívnou a objektívnou zodpovednosťou** v kontexte AI42 ....

• Analyzujte možné **scenáre zodpovednosti** v závislosti od spôsobu využitia AI (napr. ako nástroj zamestnanca, na podnikanie, v doprave, zdravotníctve)50 .

• Pri posudzovaní zodpovednosti za **omisívne konanie** v súvislosti s AI môžete použiť **Handovu formulu** (B < P × L)51 .

• **Smernica o zodpovednosti za chybné výrobky (PLD)** dopĺňa, ale nevylučuje zodpovednosť podľa Občianskeho zákonníka a **uľahčuje dokazovanie pre poškodeného**49 ....

• Oboznámte sa s **kľúčovými prvkami a úrovňami rizika AI systémov podľa AI Aktu** (zakázané praktiky, vysokorizikové, obmedzené a minimálne riziko)53 ....

• Poznajte **sankcie** za porušenie ustanovení AI Aktu54 ....

• Sledujte **časový harmonogram implementácie AI Aktu**55 ....

• **Identifikujte svoju rolu** podľa AI Aktu (poskytovateľ, nasadzujúci subjekt atď.) a zistite, či sa na vás vzťahujú jeho ustanovenia a či existujú relevantné **výnimky**57 ....

• Ak ste **poskytovateľom GPAI (všeobecných modelov AI)**, poznajte svoje povinnosti týkajúce sa **dokumentácie, informovania, dodržiavania autorských práv a zhrnutia tréningových dát**64 .... Pre GPAI so **systémovým rizikom** platia dodatočné povinnosti66 .

• Poznajte **zakázané praktiky** pri používaní AI67 ....

• Rozlišujte medzi **vysokorizikovými AI systémami ako komponentmi** určitých výrobkov (príloha I AI Aktu) a **ostatnými vysokorizikovými systémami** (príloha III AI Aktu)69 ....

• Dodržiavajte **požiadavky na transparentnosť** pre AI systémy s **obmedzeným rizikom**72 ....

pilar425.pdf - AI Act & KB ...od vágneho k určitému:

• **Vysokorizikové systémy AI musia spĺňať špecifické požiadavky** stanovené v článkoch 8 až 15 AI Aktu, týkajúce sa riadenia rizík, kvality dát, zohľadnenia zaujatosti, technickej dokumentácie, logovania, transparentnosti, ľudského dohľadu a **kybernetickej bezpečnosti**76 ....

• Poskytovatelia musia zabezpečiť **súlad AI systémov s ďalšími relevantnými právnymi predpismi EÚ**76 .

• Pri spracúvaní **osobitných kategórií údajov** musia vysokorizikové AI systémy zabezpečiť **primerané záruky**77 .

• **Technická dokumentácia** k vysokorizikovým AI systémom musí obsahovať aj **opatrenia v oblasti kybernetickej bezpečnosti**77 .

• Vysokorizikové AI systémy musia byť navrhnuté tak, aby dosahovali **primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti** počas celého ich životného cyklu79 .... To zahŕňa aj odolnosť voči poruchám a kybernetickým útokom (napr. otráveniu dát)80 .

• **Certifikácia kybernetickej bezpečnosti** podľa nariadenia (EÚ) 2019/881 môže prispieť k preukázaniu súladu s požiadavkami na kybernetickú bezpečnosť podľa AI Aktu81 .

• Do nadobudnutia účinnosti AI Aktu, **nariadenie CRA (Cyber Resilience Act)** reguluje kybernetickú bezpečnosť produktov s digitálnymi prvkami (vrátane AI) pri ich uvedení na trh EÚ82 . Aplikácia CRA nezávisí od klasifikácie AI systému podľa AI Aktu82 .

• CRA stanovuje **základné požiadavky na kybernetickú bezpečnosť**, vrátane prístupu založeného na rizikách a implementácie bezpečnostných opatrení (analýza rizík, riadenie zraniteľností, aktualizácie, ochrana pred neoprávneným prístupom, zabezpečenie dôvernosti a integrity, hlásenie incidentov)83 ....

• Pri zabezpečovaní kybernetickej bezpečnosti AI systémov je potrebné zohľadniť aj požiadavky **GDPR (čl. 32)**82 .

podskubova425.pdf - Zmluvné dojednania s IKT poskytovateľmi:

• **Zmluvy s IKT poskytovateľmi** sú kľúčové pre zabezpečenie kybernetickej bezpečnosti a ochrany dát85 ....

• Zmluva by mala jasne definovať **práva a povinnosti všetkých zúčastnených strán** v oblasti bezpečnosti86 .

• Pri uzatváraní zmlúv s tretími stranami v kontexte **Zákona o kybernetickej bezpečnosti (ZoKB)** je potrebné plniť zmluvné povinnosti a podrobiť sa dohľadu PZS/úradu13 . Vykonanie **analýzy rizík** je nevyhnutné14 .

• Pre finančný sektor, **DORA** stanovuje špecifické požiadavky na zmluvy s IKT poskytovateľmi, vrátane posúdenia rizika, komplexných zmluvných ustanovení týkajúcich sa služieb, lokalizácie dát, obnovy, auditu a ukončenia zmluvy16 ....

• V kontexte **AI Aktu** musia poskytovatelia **vysokorizikových systémov AI** prijať opatrenia na zabezpečenie ich **odolnosti** voči kybernetickým útokom91 .

• Úrad môže ukladať **sankcie** za nedodržiavanie povinností vyplývajúcich zo ZoKB91 ....

• Odporúča sa **pravidelne monitorovať legislatívny proces, revidovať zmluvnú a bezpečnostnú dokumentáciu** a zabezpečiť **asistenciu pri kontrolách a plnení notifikačných povinností**93 ....

zimen425.pdf - Právne aspekty kyber-bezpečnosti AI systémov:

• Regulácia **AI Aktu** sa primárne zameriava na **vysoko-rizikové AI systémy**, ktoré môžu predstavovať významné riziko pre zdravie, bezpečnosť alebo základné práva80 ....

• Kybernetická bezpečnosť vysokorizikových AI systémov je regulovaná prostredníctvom **AI Aktu, ZKB/NIS2, GDPR a DORA**80 ....

• **AI Akt** vyžaduje implementáciu systému riadenia rizík, data governance, technickú dokumentáciu, logovanie, návody na použitie, ľudský dohľad a **osobitné požiadavky na kybernetickú bezpečnosť**, ako je odolnosť voči poruchám a ochrana pred útokmi (otrávenie dát, oklamanie modelov)80 .

• **ZKB/NIS2** vyžadujú vykonanie **analýzy rizík** (vrátane rizík dodávateľa AI) a implementáciu **bezpečnostných opatrení**97 .

• **GDPR** vyžaduje **DPIA**, analýzu rizík a prijatie primeraných bezpečnostných opatrení, ako aj zohľadnenie princípu **privacy by design**98 .

• **DORA** sa zameriava na **digitálnu odolnosť** a riadenie rizika IKT tretích strán v finančnom sektore99 .

• Najdôležitejšie povinnosti v oblasti kybernetickej bezpečnosti závisia od **typu AI systému a úlohy subjektu** (poskytovateľ, nasadzujúci subjekt)100 .

• Identifikujte potenciálne **riziká pre AI systémy**, ako sú otrávené tréningové dáta, cielené útoky a zaujaté dáta101 ....

• Implementujte vhodné **protiopatrenia na zmiernenie týchto rizík**, napríklad kontrolu kvality dát, validáciu zdrojov, techniky na odstránenie zaujatosti, adversarial training a monitorovanie výkonnosti modelu104 ...