UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ

2026

Riadenie kybernetickej a informačnej bezpečnosti systémov umelej inteligencie správcami informačných technológií verejnej správy

(odborné stanovisko)

Projekt Kompetenčné centrum kybernetickej bezpečnosti na UPJŠ (KCKB UPJŠ) financovaný Európskou úniou z prostriedkov Plánu obnovy a odolnosti Slovenskej republiky, kód projektu: 17R05-04-V01-00007.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

OBSAH

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

1 ÚVOD

Univerzita Pavla Jozefa Šafárika v Košiciach (ďalej len „UPJŠ“) prostredníctvom Kompetenčného centra kybernetickej bezpečnosti na UPJŠ (ďalej len „KC KB UPJŠ“) pripravila odborné stanovisko k riadeniu kybernetickej a informačnej bezpečnosti systémov umelej inteligencie (ďalej len „systémy AI“) správcami informačných technológií verejnej správy (ďalej len „správcovia ITVS“).

Tento materiál poskytuje praktické odporúčania pre orgány verejnej správy pri využívaní systémov AI v rámci výkonu ich pôsobnosti. Jeho cieľom je podporiť zodpovedné, transparentné a právne konformné zavádzanie a používanie AI najmä s ohľadom na ochranu základných práv, zákonnosť rozhodovacích procesov a ochranu osobných údajov.

Materiál zároveň prispieva k zvyšovaniu právnej istoty a jednotnosti postupov pri implementácii AI riešení vo verejnom sektore. Poskytuje rámcové odporúčania pre identifikáciu vhodných oblastí využitia AI, hodnotenie rizík spojených s jej nasadením a nastavenie interných procesov, kontrolných mechanizmov a zodpovedností pri jej používaní, pričom reflektuje princípy riadenia bezpečnosti podľa právnej úpravy a všeobecne používaných štandardov ako ISO/IEC 27001 a ISO/IEC 42001.

Odborné stanovisko vytvára orientačný rámec pre bezpečné a etické využívanie AI vo verejnej správe a podporuje modernizáciu verejných služieb pri zachovaní dôvery verejnosti. Súčasťou materiálu je aj prehľad odporúčaných bezpečnostných opatrení vychádzajúcich z modelu PDCA (Plan–Do–Check–Act), ktoré môžu správcovia ITVS aplikovať pri riadení bezpečnosti systémov AI.

Toto odborné stanovisko má nezáväzný a odporúčací charakter. Predstavuje jeden z možných prístupov k riadeniu využívania AI vo verejnej správe a slúži ako metodická pomôcka pre jeho praktickú aplikáciu. Nenahrádza platnú právnu úpravu ani záväzné stanoviská alebo metodické usmernenia orgánov verejnej moci, ktoré majú danú problematiku v gescii.

V rámci predloženej analýzy sme vychádzali z nasledujúcich legislatívnych východísk, ktoré predstavujú základný normatívny rámec:

- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „zákon o ZoITVS“),
- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej aj „ZoKB“),
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (ďalej aj „AI akt“),
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej aj „GDPR“).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

2 VZŤAH AI A INFORMAČNÝCH TECHNOLÓGIÍ VEREJNEJ SPRÁVY

V tejto kapitole uvádzame základné legálne definície pojmov, s ktorými tento dokument ďalej pracuje, aby bol zabezpečený ich jednotný výklad v právnom aj aplikačnom kontexte. Vymedzenie týchto pojmov vychádza z právnych aktov Európskej únie. Osobitná pozornosť sa venuje aj pojmom, ktoré sú kľúčové pre bezpečné, zákonné a zodpovedné navrhovanie, nasadzovanie a používanie systémov AI. Cieľom tejto časti je vytvoriť terminologický základ pre ďalšiu analýzu právneho postavenia systémov AI vo verejnej správe.

2.1 VYMEDZENIE ZÁKLADNÝCH POJMOV

Prevádzkové údaje: údaje získané počas prevádzkovej fázy systému AI, na základe ktorých nasadený systém AI vypočítava výstup (prevzaté z ISO/IEC 22989:2022).

Osobné údaje: sú osobné údaje v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679 (prevzaté z čl. 50 AI Aktu).

Osobitné kategórie osobných údajov: sú kategórie osobných údajov uvedené v článku 9 ods. 1 nariadenia (EÚ) 2016/679, článku 10 smernice (EÚ) 2016/680 a článku 10 ods. 1 nariadenia (EÚ) 2018/1725 (prevzaté z čl. 37 AI Aktu).

Iné ako osobné údaje: sú údaje iné než osobné údaje v zmysle vymedzenia v článku 4 bode 1 nariadenia (EÚ) 2016/679 (prevzaté z čl. 51 AI Aktu).

Systém AI: je strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie (prevzaté z čl. 1 AI Aktu).

Riziko: je kombinácia pravdepodobnosti výskytu ujmy a závažnosti tejto ujmy (prevzaté z čl. 2 AI Aktu).

Poskytovateľ: je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý vyvíja systém AI alebo model AI na všeobecné účely alebo ktorý si dáva vyvinúť systém AI alebo model AI na všeobecné účely a uvádza ho na trh alebo uvádza systém AI do prevádzky pod svojím vlastným menom alebo ochrannou známkou, či už za odplatu alebo bezodplatne (prevzaté z čl. 3 AI Aktu).

Nasadzujúci subjekt: je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý používa systém AI v rámci svojej právomoci, s výnimkou prípadov, keď sa systém AI používa v rámci osobnej neprofesionálnej činnosti (prevzaté z čl. 4 AI Aktu).

Výkon systému AI: je schopnosť systému AI dosiahnuť jeho zamýšľaný účel (prevzaté z čl. 18 AI Aktu).

Gramotnosť v oblasti AI: sú zručnosti, vedomosti a pochopenie, ktoré poskytovateľom, nasadzujúcim subjektom a dotknutým osobám umožňujú s ohľadom na ich príslušné práva a povinnosti v kontexte tohto nariadenia informovane nasadzovať systémy AI, ako aj získať povedomie o príležitostiach a rizikách AI a o prípadnej ujme, ktorú môže spôsobiť (prevzaté z čl. 56 AI Aktu).

Zaujatosť (bias): systematický rozdiel v zaobchádzaní s určitými objektmi, osobami alebo skupinami v porovnaní s inými; zdrojom zaujatosti môžu byť tréningové dáta, kognitívne skreslenia pri ich zbere, ako aj inžinierske rozhodnutia pri vývoji systému (prevzaté z ISO/IEC 22989:2022, čl. 3.5.4).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Vysvetliteľnosť: vlastnosť systému AI vyjadriť dôležité faktory ovplyvňujúce výsledky systému AI spôsobom zrozumiteľným pre ľudí (prevzaté z ISO/IEC 22989:2022, čl. 3.5.7).

Implementácia/nasadenie systému AI: inštalácia, vydanie alebo konfigurácia systému AI na prevádzku v cieľovom prostredí (prevzaté z ISO/IEC 22989:2022, čl. 6.2.5).

2.2 PRÁVNE POSTAVENIE SYSTÉMOV AI PODĽA ZOITVS

Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v ustanovení § 2 upravuje základné definície. Na účely predmetného zákona uvádza definície:

- **informačnej technológie**, za ktorú považuje prostriedok alebo postup, ktorý slúži na spracúvanie údajov alebo informácií v elektronickej podobe, najmä informačný systém, infraštruktúra, informačná činnosť a elektronické služby (§2 ods. 1 ZoITVS),
- **informačného systému**, za ktorý považuje funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov (§2 ods. 2 ZoITVS).

Okrem týchto definícii predmetné ustanovenie dopĺňa aj právne definície pojmov informačná technológia verejnej správy a informačný systém verejnej správy:

- **informačnou technológiou verejnej správy** sa rozumie informačná technológia v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby. Na účely tohto zákona sa povinnosti v rámci správy informačných technológií verejnej správy vzťahujú aj na údaje, procesné postupy, personálne zabezpečenie a organizačné zabezpečenie, ak tvoria funkčný celok alebo ak samy osebe slúžia na spracúvanie údajov alebo informácií v elektronickej podobe (§2 ods. 3 ZoITVS),
- **informačným systémom verejnej správy** sa rozumie informačný systém v pôsobnosti správcu podporujúci služby verejnej správy, služby vo verejnom záujme alebo verejné služby (§2 ods. 4 ZoITVS).

Okrem vyššie uvedených definícii ZoITVS uvádza aj legálne definície subjektov, ktoré vykonávajú činnosti k informačným systémom verejnej správy alebo informačných technológiám verejnej správy. Na účely ZoITVS ide o tieto subjekty:

- **správcom** je ten orgán riadenia, ktorého za správcu informačnej technológie verejnej správy ustanoví zákon alebo je ustanovený na základe ZoITVS. Ak zákon vo vzťahu k informačnej technológii verejnej správy správcu neustanovuje, je správcom na účely ZoITVS ten orgán riadenia, ktorý informačnú technológiu verejnej správy používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby; ak je takýchto orgánov riadenia viac a jedným z nich je aj ústredný orgán štátnej správy, správcom je tento ústredný orgán štátnej správy (§2 ods. 5 ZoITVS).
- **prevádzkovateľom** je správca, osobitným predpisom ustanovený orgán riadenia alebo správcom určená osoba. Správcom určený alebo osobitným predpisom ustanovený prevádzkovateľ vykonáva, v rozsahu povinností správcu, činnosti, ktoré mu určí správca alebo ustanoví tento osobitný predpis; ak tento osobitný predpis rozsah činností prevádzkovateľa neustanovuje, vykonáva ich v celom rozsahu činností správcu. Určením alebo ustanovením

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

prevádzkovateľa nie je dotknutá zodpovednosť správcu za plnenie povinností podľa ZoITVS (§2 ods. 6 ZoITVS).

Definíciu **systému AI** nachádzame v článku 3 bod 1 Nariadenia Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (ďalej len „Akt o AI“). Podľa tohto článku systém AI je strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie;

Systém AI predstavuje prostriedok na spracúvanie údajov alebo informácií v elektronickej podobe. V porovnaní so všeobecnými informačnými technológiami systém AI rozširuje tento pojem o schopnosť adaptívneho spracovania a generovania výstupov na základe dát. Z pohľadu vyššie uvedeného a právnej regulácie ide teda o špecifickú podmnožinu **informačných technológií** s vyššou mierou autonómnosti. V prípade ak by takýto systém AI bol v pôsobnosti správcu podporujúca služby verejnej správy, služby vo verejnom záujme alebo verejné služby, možno takýto systém AI považovať za **informačnú technológiu verejnej správy**.

Systém AI sa stáva informačnou technológiou verejnej správy v momente, keď je používaný správcom na poskytovanie verejných služieb. Ak AI systém tvorí alebo je súčasťou informačného systému, ktorý podporuje verejné služby, možno ho kvalifikovať ako **informačný systém verejnej správy.**

V praxi môžu existovať viaceré prípady použitia systémov AI (zaradenie bude závisieť od miery integrácie a vplyvu na poskytovanie služby):

- systém AI ako súčasť informačného systému verejnej správy (napr. chatbot pre komunikáciu s občanmi),
- systém AI ako podporný modul (napr. analytický komponent),
- systém AI ako samostatný informačný systém verejnej správy (napr. autonómny rozhodovací systém).

Správcom systému AI je podľa § 2 ods. 5 ZoITVS orgán verejnej správy, ktorý systém AI používa na účely poskytovania služby verejnej správy, služby vo verejnom záujme alebo verejnej služby. Správca systému AI zodpovedá za plnenie povinností podľa ZoITVS. **Prevádzkovateľom systému AI** podľa § 2 ods. 6 ZoITVS môže byť:

- samotný správca systému AI,
- správcom AI určená osoba – externý dodávateľ (napr. cloudová AI služba),
- poverená organizácia.

Delegovanie činností na prevádzkovateľa systému AI nemení zodpovednosť správcu systému AI v zmysle §2 ods. 6 ZoITVS. Ide o dôležité ustanovenie, keďže pri systémoch AI systémoch dochádza k outsourcingu modelov alebo infraštruktúry (napr. LLM API). Vzniká tak potreba jasného rozdelenia rolí a riadenia dodávateľského reťazca.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

3 VYBRANÉ PRÁVNE ASPEKTY

Pri implementácii systémov umelej inteligencie orgánmi verejnej správy je nevyhnutné vychádzať z premisy, že implementácia týchto systémov nie je len otázkou technologickej modernizácie, ale predovšetkým otázkou dôsledného dodržiavania právnych predpisov. Každé nasadenie systému AI v prostredí verejnej správy predstavuje výkon verejnej moci, ktorý musí byť zákonný a musí sa opierať o jasný, predvídateľný a kontrolovateľný právny rámec.

Využívanie systémov AI je preto potrebné posudzovať najmä z hľadiska ich súladu s platnou legislatívou, pričom osobitný dôraz sa kladie na ochranu základných práv a slobôd dotknutých osôb. Ide najmä o dodržiavanie pravidiel ochrany osobných údajov, zabezpečenie spravodlivého a nestranného rozhodovania, rešpektovanie zákazu diskriminácie, ako aj garanciu transparentnosti a preskúmateľnosti postupov orgánov verejnej správy.

Analytický materiál vychádza z predpokladu, že orgány verejnej správy vystupujú pri používaní systémov AI spravidla v postavení prevádzkovateľov spracúvania osobných údajov, a preto nesú primárnu zodpovednosť za zabezpečenie súladu ich využívania s právnymi predpismi. Zároveň je potrebné zdôrazniť, že systémy AI nemôžu nahrádzať rozhodovaciu činnosť orgánov verejnej správy bez zachovania zákonných garancií, najmä pokiaľ ide o preskúmateľnosť rozhodnutí, možnosť zásahu človeka a ochranu práv dotknutých osôb.

3.1 DÁTA A OCHRANA OSOBNÝCH ÚDAJOV

Využívanie systémov umelej inteligencie (AI) orgánmi verejnej správy prináša významné možnosti zefektívnenia výkonu verejnej moci, automatizácie administratívnych procesov, podpory rozhodovania a zlepšenia poskytovania verejných služieb. Súčasne však predstavuje aj zvýšené riziká z pohľadu ochrany osobných údajov, najmä ak sú systémy umelej inteligencie využívané pri spracúvaní údajov fyzických osôb. Orgány verejnej správy sú preto pri implementácii a používaní systémov AI povinné zabezpečiť, aby spracúvanie osobných údajov prebiehalo v súlade s právnymi predpismi na ochranu osobných údajov, najmä s Nariadením Európskeho parlamentu a Rady (EÚ) 2016/679 (GDPR) a príslušnými vnútroštátnymi právnymi predpismi.

Pri používaní systémov AI platia rovnaké pravidlá ako pri inej práci s údajmi. Akékoľvek nahratie textu a lebo dokumentu do systému AI sa považuje za spracovanie osobných údajov. To znamená, že za ne zodpovedá osoba, ktorá ich do nástroja vložila — nie model.

3.1.1 ZÁSADY SPRACÚVANIA OSOBNÝCH ÚDAJOV PRI VYUŽÍVANÍ AI

Pri používaní AI nástrojov v rámci výkonu verejnej správy musia orgány verejnej správy rešpektovať základné zásady spracúvania osobných údajov. Ide najmä o zásadu zákonnosti, spravodlivosti a transparentnosti, zásadu minimalizácie údajov, zásadu obmedzenia účelu, zásadu presnosti údajov, zásadu obmedzenia uchovávania a zásadu integrity a dôvernosti.

Pri implementácii AI systémov je potrebné osobitne dbať na to, aby:

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- osobné údaje boli spracúvané len v rozsahu nevyhnutnom na dosiahnutie zákonom stanoveného účelu,
- účel spracúvania bol jasne definovaný a kompatibilný s právnym základom spracúvania,
- AI systémy nevyužívali osobné údaje spôsobom, ktorý by bol nezlučiteľný s pôvodným účelom ich získania,
- bolo zabezpečené primerané technické a organizačné zabezpečenie spracúvania údajov.

Pri zásade minimalizácii údajov bude nevyhnutné si určiť, ktoré údaje sú nevyhnutné, ako limit pre tréningové, testovacie a prevádzkové dáta modelu.

3.1.2 PRÁVNY ZÁKLAD SPRACÚVANIA OSOBNÝCH ÚDAJOV PRI VYUŽÍVANÍ AI

To, aký je právny základ spracúvania osobných údajov pri využívaní AI stanovuje nariadenie GDPR.

Orgány verejnej správy môžu spracúvať osobné údaje prostredníctvom AI nástrojov len v prípade, ak existuje relevantný právny základ spracúvania. V podmienkach verejnej správy pôjde najčastejšie o:

- plnenie zákonnej povinnosti prevádzkovateľa,
- plnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci,
- v niektorých prípadoch súhlas dotknutej osoby, ak ide o doplnkové služby alebo dobrovoľné nástroje.

Pri využívaní AI systémov je nevyhnutné posúdiť, či právny základ pokrýva aj automatizované spracúvanie alebo profilovanie, ak je takýto typ spracúvania súčasťou fungovania daného systému.

3.1.3 POSÚDENIE VPLYVU NA OCHRANU OSOBNÝCH ÚDAJOV (DPIA)

V zmysle čl. 35 ods. 1 nariadenia GDPR *ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie.* Povinnosť vykonať posúdenie vplyvu na ochranu osobných údajov (Data Protection Impact Assessment – DPIA) v zmysle tohto článku nariadenia môže vzniknúť najmä pri:

- využívaní AI systémov na automatizované rozhodovanie,
- profilovaní fyzických osôb,
- spracúvaní veľkého objemu osobných údajov,
- spracúvaní osobitných kategórií osobných údajov,
- systematickom monitorovaní správania osôb.

Cieľom DPIA je identifikovať potenciálne riziká pre dotknuté osoby a navrhnúť opatrenia na ich minimalizáciu ešte pred nasadením AI systému do praxe.

3.1.4 TRANSPARENTNOSŤ A INFORMOVANIE DOTKNUTÝCH OSÔB

Orgány verejnej správy sú povinné zabezpečiť transparentnosť spracúvania osobných údajov aj v prípadoch, keď sú údaje spracúvané prostredníctvom AI nástrojov. Uvedené úzko súvisí s aplikáciou

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ustanovení nariadenia GDPR o právach dotknutých osôb v zmysle čl. 12 – 22. Dotknuté osoby by mali byť primerane informované najmä o:

- tom, že pri spracúvaní údajov môže byť využívaný systém umelej inteligencie,
- účele takéhoto spracúvania,
- právnom základe spracúvania,
- rozsahu spracúvaných údajov,
- prípadnom automatizovanom rozhodovaní alebo profilovaní.

Informácie by mali byť poskytované jasným, zrozumiteľným a ľahko dostupným spôsobom, napríklad prostredníctvom informačných povinností podľa GDPR alebo prostredníctvom interných portálov a webových sídiel orgánov verejnej správy.

3.1.5 AUTOMATIZOVANÉ ROZHODOVANIE A ĽUDSKÝ DOHĽAD

Ak je AI systém využívaný na podporu alebo realizáciu rozhodovania orgánov verejnej správy, je potrebné zabezpečiť primeraný ľudský dohľad nad rozhodovacím procesom. Rozhodnutia, ktoré majú právne účinky alebo významne ovplyvňujú dotknuté osoby, by nemali byť prijímané výlučne automatizovaným spôsobom bez možnosti ľudského zásahu, pokiaľ to právny predpis výslovne neumožňuje.

Orgány verejnej správy by mali zabezpečiť, aby:

- konečné rozhodnutie bolo preskúmateľné a postup, ktorý prechádzal vydaniu rozhodnutia musí byť transparentný
- existovala možnosť ľudského zásahu do rozhodovacieho procesu,
- dotknuté osoby mali možnosť napadnúť alebo preskúmať automatizované rozhodnutie.

V súvislosti s uvedeným sa odporúča vytvoriť postup, ako poskytnúť zrozumiteľné vysvetlenie výsledku rozhodnutia systému umelej inteligencie a ako zabezpečiť prehodnotenie rozhodnutia človekom, ak o to osoba požiada.

3.1.6 BEZPEČNOSŤ SPRACÚVANIA A VÝBER SYSTÉMOV AI

Pri výbere a implementácii systémov AI je potrebné venovať zvýšenú pozornosť bezpečnosti spracúvania osobných údajov, na ktorú poukazuje čl. 32 nariadenia. Požiadavky na bezpečnosť, odolnosť a kybernetickú bezpečnosť vysokorizikových systémov stanovuje čl. 15 Aktu AI. Orgány verejnej správy by mali preveriť najmä:

- spôsob ukladania a prenosu údajov,
- lokalizáciu dátových centier,
- podmienky spracúvania údajov poskytovateľom AI služby,
- existenciu zmluvného vzťahu so sprostredkovateľom spracúvania.

Odporúča sa, aby orgán verejnej moci rozšíril bezpečnostné opatrenia aj na modely a tréningové dáta (prístupové práva, oddelenie prostredí, vedenie záznamov o práci s modelom). Odporúča sa tiež zahrnúť do bezpečnostnej analýzy špecifické hrozby pre systémy umelej inteligencie (útoky cez vstupy, pokusy získať tréningové dáta z modelu, manipulácia výstupov). Osobitne chrániť citlivé údaje.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ak je AI nástroj poskytovaný externým dodávateľom, je potrebné zabezpečiť uzavretie zmluvy o spracúvaní osobných údajov podľa čl. 28 GDPR.

3.1.7 INTERNÉ PRAVIDLÁ POUŽÍVANIA SYSTÉMOV AI

Orgány verejnej správy by mali prijať interné pravidlá upravujúce používanie systémov AI zamestnancami. Tieto pravidlá by mali obsahovať najmä:

- zákaz zadávania osobných údajov do verejne dostupných systémov AI bez právneho a bezpečnostného posúdenia,
- pravidlá anonymizácie alebo pseudonymizácie údajov pri využívaní systémov AI,
- pravidlá používania generatívnych systémov AI,
- postupy kontroly a auditu používania systémov AI.

Takéto interné pravidlá prispievajú k minimalizácii rizika neoprávneného spracúvania osobných údajov a k zabezpečeniu súladu využívania systémov AI s právnymi predpismi.

3.2 ZODPOVEDNOSŤ A DOHĽAD

Za súlad využívania nástrojov umelej inteligencie so zásadami ochrany osobných údajov nesie plnú zodpovednosť príslušný orgán verejnej správy v postavení prevádzkovateľa spracúvania osobných údajov. Táto zodpovednosť nie je len formálna, ale zahŕňa aktívnu povinnosť zabezpečiť, aby všetky fázy spracúvania osobných údajov prostredníctvom AI nástrojov – od ich získavania, cez analýzu až po uchovávanie či ďalšie využitie – prebiehali v súlade s relevantnou právnou úpravou, najmä s požiadavkami nariadenia GDPR a súvisiacich predpisov. Prevádzkovateľ je povinný už vo fáze výberu a implementácie AI nástroja posúdiť jeho vplyv na ochranu osobných údajov. Zároveň musí zabezpečiť, aby boli dodržané základné zásady spracúvania osobných údajov, ako sú zákonnosť, správnosť, minimalizácia údajov, či obmedzenie účelu.

Súčasťou tejto zodpovednosti je aj nastavenie primeraných technických a organizačných opatrení, ktoré reflektujú špecifiká využívania AI, vrátane rizík spojených s automatizovaným rozhodovaním, profilovaním alebo možnými diskriminačnými dopadmi algoritmov.

Priebežný dohľad nad využívaním AI nástrojov predstavuje nevyhnutný prvok zodpovedného riadenia týchto technológií. Nejde pritom o jednorazovú kontrolu, ale o kontinuálny proces monitorovania, ktorý zahŕňa pravidelné preverovanie súladu používaných nástrojov s právnymi a etickými požiadavkami. Orgány verejnej správy by mali zaviesť interné kontrolné mechanizmy, vrátane určenia zodpovedných osôb alebo útvarov (napr. zodpovednej osoby pre ochranu osobných údajov), ktoré budú dohliadať na používanie AI nástrojov pri výkone činnosti.

Rovnako dôležité je pravidelné hodnotenie rizík spojených s využívaním AI nástrojov. Technologické prostredie sa dynamicky vyvíja a riziká, ktoré neboli identifikované pri zavedení systému, sa môžu prejaviť až v jeho aplikačnej praxi. Preto je potrebné vykonávať opakované analýzy rizík, ktoré zohľadňujú nové okolnosti, zmeny v legislatíve či vývoj samotných AI systémov. Na základe týchto hodnotení by mali byť prijímané adekvátne opatrenia na zmiernenie identifikovaných rizík.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Neoddeliteľnou súčasťou tohto procesu je aj priebežná aktualizácia interných pravidiel a metodických usmernení. Tieto dokumenty by mali reflektovať aktuálny stav právnej úpravy, technologický pokrok, ako aj praktické skúsenosti z využívania AI v konkrétnych agendách verejnej správy. Ich cieľom je poskytnúť zamestnancom jasné a zrozumiteľné pravidlá pre používanie AI nástrojov, čím sa minimalizuje riziko nezákonného alebo neetického spracúvania osobných údajov.

Komplexné nastavenie dohľadu, hodnotenia rizík a interných pravidiel tak predstavuje kľúčový predpoklad pre to, aby využívanie umelej inteligencie vo verejnej správe prebiehalo nielen efektívne, ale predovšetkým v súlade s požiadavkami ochrany základných práv a slobôd fyzických osôb, vrátane práva na ochranu osobných údajov.

3.3 ZMLUVNÁ AGENDA

Možnosti nadobudnutia produktu využívajúceho AI na základe zmluvy od externých subjektov (dodávateľov) možno realizovať:

1) získaním existujúceho produktu alebo
2) objednaním vytvorenia takéhoto produktu a dodania dodávateľom.

V obidvoch prípadoch je potrebné zrealizovať proces v súlade s pravidlami verejného obstarávania podľa zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov a v rámci pravidiel obstarávania a implementácie informačných technológií verejnej správy v súlade so zákonom č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

Získanie existujúceho produktu s integrovanými prvkami AI

V rámci zmluvných vzťahov môže ísť o **nepomenovanú zmluvu,** ktorá bude zohľadňovať komplexnosť vzťahov, vrátane licenčných a servisných podmienok. Zmluvu zrejme predloží dodávateľ produktu AI a mohlo by ísť o zmluvu s náležitosťami, ktoré štandardne obsahujú licenčné a servisné zmluvy na počítačové programy.

Vytvorenie produktu s integrovanými prvkami AI na základe požiadavky objednávateľa

Aj v tomto prípade pôjde zmiešanú nepomenovanú zmluvu, ktorá bude navyše, v porovnaní s predošlým prípadom, obsahovať ustanovenia o vytvorení produktu AI.

Keďže v prípade vytvorenia produktu AI na mieru predpokladáme väčšiu mieru ingerencie objednávateľa (OVM) v procese kontraktácie, odporúčame:

- Sústrediť sa na identifikáciu problému a dôvody zavedenia produktu AI v organizácii, identifikovať požiadavky na informačné technológie a podmienky ich zabezpečenia, nastaviť požiadavky prevádzky pre všetky informačné technológie verejnej správy, ktoré sú súčasťou projektu. Identifikovať požiadavky s ohľadom na potreby koncových používateľov, dostupné kapacity informačných technológií a ľudských zdrojov. Požiadavky na architektúru informačných technológií verejnej správy musia byť v súlade s centrálnou architektúrou.
- Identifikáciu predmetu a účelu zmluvy. Podrobný opis predmetu a jeho fungovania s flexibilným dopĺňaním počas vývoja (agilný vývoj).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- Identifikovať požiadavky, riziká, prínosy a merateľné kritériá kvality.
- Jasne komunikovať dátovú stratégiu organizácie a požiadavky na fungovanie a vlastnosti produktu.
- Komunikovať kvalitu dodávaných údajov (vrátane údajov a dát chránených právami tretích osôb; napr. osobné údaje, predmety duševného vlastníctva). OVM by mal jasne definovať a zmluvne garantovať určité vlastnosti údajov, ktoré poskytuje dodávateľovi, najmä údaje o pôvode (t. j. či ide o vlastné dáta, verejné zdroje, dáta tretích osôb), právny režim údajov (t. j. či obsahujú osobné údaje chránené podľa GDPR), predmety chránené autorským právom (najmä texty, databázy, obrázky, počítačové programy), obchodné tajomstvo vrátane know-how alebo dôverné informácie, kvalitu a presnosť dát (najmä aktuálnosť, úplnosť, reprezentatívnosť, čo je dôležité aj pre trénovanie systémov AI), licenčné oprávnenia udelené objednávateľovi s informáciou, či má objednávateľ právo dáta poskytnúť na účely vývoja AI produktu. Zmluvy by mal riešiť otázku zodpovednosti za legalitu dát, definovať zakázané typy dát (napr. neanonymizované osobné údaje), povinnosť anonymizovať alebo pseudonymizovať údaje. Za účelom eliminovania rizika zneužitia údajov zo strany dodávateľa, odporúčame poskytovať fiktívne údaje pri tvorbe produktu AI alebo pri vývoji a testovaní systému používať syntetické údaje alebo anonymizované datasety.
- V prípade poskytnutia reálnych údajov zabezpečiť mlčanlivosť dodávateľa a jeho zamestnancov alebo tretích osôb (napr. subdodávateľov). Bezpečnostné opatrenia môžu spočívať v technických opatreniach, napr. šifrovanie dát alebo organizačných opatreniach, napr. Školenia, interné politiky, podpisovanie dohôd o mlčanlivosti, ukladanie sankcií za porušenie.
- Formulovať požiadavky na kvalitu výstupov.
- Preniesť v plnej miere riziko porušenia práv tretích osôb (vrátane práv DV) a zodpovednosť za toto porušenie na dodávateľa.
- Komunikovať etické zásady využívania AI, prípadne oboznámiť dodávateľa so sektorovými pravidlami etických štandardov.
- Komunikovať požiadavky na kompatibilitu a interoperabilitu s existujúcimi technológiami využívanými v organizácii.
- Formulovať poskytovanie servisných služieb a údržbu systému počas trvania zmluvného vzťahu s osobitným dôrazom na bezpečnosť informačných technológií.
- Aj po skončení platnosti zmluvy zabezpečiť údržbu systému a jeho fungovanie na účel, na ktorý bol vytvorený, zabezpečiť právnu a technickú kontinuitu fungovania systému, vrátane prevádzky, servisu a podpory informačných technológií verejnej správy zabezpečovaných tretími osobami.
- Eliminovať vznik závislosti od dodávateľa po skončení zmluvy.
- Dohodnúť finálnu odmenu za produkt a čas jeho vytvorenia. Pri postupnom vytváraní dohodnúť časové míľniky vrátane priebežnej kontroly plnenia zmluvy a testovania produktu určenými osobami. Pri postupnom plnení predmetu zmluvy odporúčame dohodnúť cenu podľa rozpočtu. Do ceny zahrnúť aj prípadné licenčné poplatky a náklady na údržbu systému počas trvania zmluvy a po skončení zmluvy.
- Vo fáze implementácie zabezpečovať riadenie zmien a udržiavať technické informácie o realizovanom riešení v aktuálnom a správnom stave vrátane informácií o väzbách medzi jednotlivými jeho prvkami.
- Dohodnúť nakladanie s právami duševného vlastníctva vrátane tzv. preexistentného duševného vlastníctva dodávateľa a objednávateľa, duševného vlastníctva vytvoreného individuálne dodávateľom alebo objednávateľom a duševného vlastníctva vytvoreného spoločne dodávateľom a objednávateľom.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- Pri formulovaní zmluvných podmienok zohľadniť čo najväčší rozsah práv na použitie pre objednávateľa smerom k verejnosti, vrátane zverejnenia produktu (napr. zdrojového kódu počítačového programu) v prípade financovania z verejných zdrojov.
- Pred finálnym odovzdaním zabezpečiť primeraný čas na testovanie produktu a po odovzdaní precizovať záruky a zodpovednosť za vady v záručnej dobe vrátane pozáručného servisu.

Správca je na úseku obstarávania a implementácie informačných technológií verejnej správy povinný akceptovať len také zmluvné podmienky, podľa ktorých:

1) zdrojový kód vytvorený počas projektu bude otvorený v súlade s licenčnými podmienkami verejnej softvérovej licencie Európskej únie podľa osobitného predpisu,18) a to v rozsahu, v akom zverejnenie tohto kódu nemôže byť zneužité na činnosť smerujúcu k narušeniu alebo k zničeniu informačného systému verejnej správy,
2) je jediným a výhradným disponentom so všetkými informáciami zhromaždenými alebo získanými počas projektu a prevádzky projektom vytvoreného riešenia vrátane jeho zmien a servisu a
3) pri zmene dodávateľa pôvodný dodávateľ poskytne správcovi úplnú súčinnosť pri prechode na nového dodávateľa, najmä v oblasti architektúry a integrácie informačných systémov.

3.4 PRÁVO DUŠEVNÉHO VLASTNÍCTVA

Právo duševného vlastníctva zahŕňa autorské právo, právo príbuzné autorskému právu (práva výkonných umelcov) a práva súvisiace s autorským právom (práva výrobcov zvukových záznamov, audiovizuálnych záznamov, vysielateľov, vydavateľov periodík a práva k databázam *sui generis*) a tiež práva priemyselného vlastníctva (patentové právo, právo úžitkových vzorov, dizajnov, topografií polovodičových výrobkov a odrôd rastlín a tiež právo ochranných známok, označení pôvodu výrobkov a zemepisných označení výrobkov, či právo obchodných mien), práva obdobné priemyselným právam (právo zlepšovacích návrhov, nových spôsobov prevencie, diagnostiky chorôb a liečenia ľudí a zvierat a ochrany rastlín proti škodcom a chorobám, právo know-how, doménové mená a logo).

Medzi predmety duševného vlastníctva potenciálne najviac dotknuté využívaním systémov AI patria autorské diela vrátane počítačových programov, či databáz. Podľa § 3 ods. 1 Autorského zákona (zákon č. 185/2015 Z .z. v znení neskorších predpisov) je predmetom autorského práva dielo z oblasti literatúry, umenia alebo vedy, ktoré je jedinečným výsledkom tvorivej duševnej činnosti autora vnímateľným zmyslami, bez ohľadu na jeho podobu, obsah, kvalitu, účel, formu jeho vyjadrenia alebo mieru jeho dokončenia.

V snahe predísť zásahom do práv duševného vlastníctva bude potrebné dbať na legalitu primárneho zdroja a zabezpečiť vysporiadanie práv duševného vlastníctva, čo by malo byť povinnosťou dodávateľa systému AI.

Výstupy vytvorené AI podľa platnej legislatívy nie je možné považovať za autorské diela a poskytnúť im autorskoprávnu ochranu.

Príklady:

1. Orgán verejnej správy začne využívať generatívny AI nástroj na prípravu analytických správ a metodických materiálov. Následne sa zistí, že niektoré výstupy obsahujú texty a obrázky, ktoré

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

sú veľmi podobné materiálom z odborných publikácií a databáz, ku ktorým inštitúcia nemá licenciu.

2. Orgán verejnej správy využije AI nástroj na generovanie grafického návrhu informačnej kampane (plagáty, vizuály na sociálne siete). Po zverejnení sa autor fotografie ozve, že výsledný vizuál výrazne vychádza z jeho autorského diela, ktoré bolo použité bez súhlasu a licencie. Inštitúcia zároveň nevie preukázať pôvod dát, na ktorých bol AI model trénovaný, ani rozsah oprávnenia na použitie výstupov.
3. Orgán verejnej správy využije AI nástroj na automatické preklady a spracovanie odborných dokumentov vrátane chránených autorských diel. Preklad a spracovanie cudzieho diela pritom predstavuje autorskoprávne relevantné použitie diela. Následne sa ukáže, že systém spracúva aj chránené publikácie a vytvára z nich preklady alebo zhrnutia, ktoré sú ďalej distribuované bez súhlasu nositeľov práv. Tým môže dochádzať k neoprávnenému rozmnožovaniu a sprístupňovaniu autorských diel.

V uvedených príkladoch vzniká riziko porušenia autorských práv alebo licenčných podmienok pri ďalšom zverejnení alebo použití týchto materiálov.

3.5 ETICKÉ ASPEKTY

Využívanie AI so sebou prináša aj **etické otázky** používania a možného zneužitia AI v inštitúcii.

Vzhľadom na osobitosti etických problémov je vhodná sektorová formulácia etických princípov s ohľadom na oblasť pôsobnosti orgánov verejnej správy. Za prínosné tiež považujeme prijatie interných etických noriem používania AI v inštitúcii a zriadenie etickej komisie pre posudzovanie etických dôsledkov používania AI. Pokiaľ organizácia má etickú komisiu, je možné rozšíriť jej kompetencie aj o oblasť AI. Predpokladáme, že bude potrebné zorganizovať aj vzdelávanie členov komisie s ohľadom na nový okruh pôsobnosti.

Etické problémy často zrkadlia aj nastolené právne otázky a preto bude vhodné ich riešiť aj za účasti právnikov, resp. iných odborníkov na AI.

Príklady:

1. V praxi by mohli nastať situácie, keď orgán verejnej správy začne využívať komerčný systém umelej inteligencie na automatizované predbežné posudzovanie žiadostí o sociálnu dávku. Po niekoľkých mesiacoch sa objavia podnety občanov a mimovládnych organizácií, že systém častejšie označuje žiadosti z určitých regiónov alebo sociálnych skupín ako „rizikové“, pričom nie je jasné, podľa akých kritérií k tomu dochádza. Zároveň nie je možné žiadateľom zrozumiteľne vysvetliť dôvody negatívneho hodnotenia systému, čo vyvoláva otázky transparentnosti rozhodovania a možného porušenia zásady spravodlivosti. Etická komisia má posúdiť, či používanie systému nevedie k diskriminačným výsledkom, či je zabezpečená primeraná ochrana osobných údajov a či je potrebné upraviť alebo pozastaviť jeho používanie.
2. Orgán verejnej správy nasadí AI nástroj na automatické triedenie podnetov občanov a určovanie ich priority. Postupne sa ukáže, že systém uprednostňuje podania formulované formálnejším jazykom, čím znevýhodňuje niektoré skupiny obyvateľstva, pričom kritériá hodnotenia nie sú transparentné. Alebo systém tematicky uprednostňuje podnety, ktoré sú menej “konfliktné”. Etická komisia má posúdiť, či systém neporušuje princípy spravodlivosti, transparentnosti a ochrany súkromia a navrhnúť opatrenia na jeho úpravu alebo obmedzenie.
3. Orgán verejnej správy využíva AI systém na hodnotenie uchádzačov o zamestnanie vo verejnej službe (napr. za účelom selekcie kandidátov, ktorí budú pozvaní na pohovor). Následne sa

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

objavia podozrenia, že algoritmus systematicky znevýhodňuje starších uchádzačov alebo ženy - matky, pričom rozhodovacie kritériá nie sú vysvetlené. Zároveň nie je jasné, z akých dát bol systém trénovaný a či boli použité údaje v súlade s ochranou osobných údajov. Etická komisia má posúdiť diskriminačné riziká, mieru transparentnosti a zákonnosť spracúvania údajov a odporučiť ďalší postup.

Rovnaké riziko hrozí aj pri nasadení AI agentov v rámci inštitúcií, preto je nevyhnutné podrobiť každé rozhodovanie ľudskej kontrole a posúdiť súladnosť so zákonom vrátane interných predpisov o etickom používaní AI.

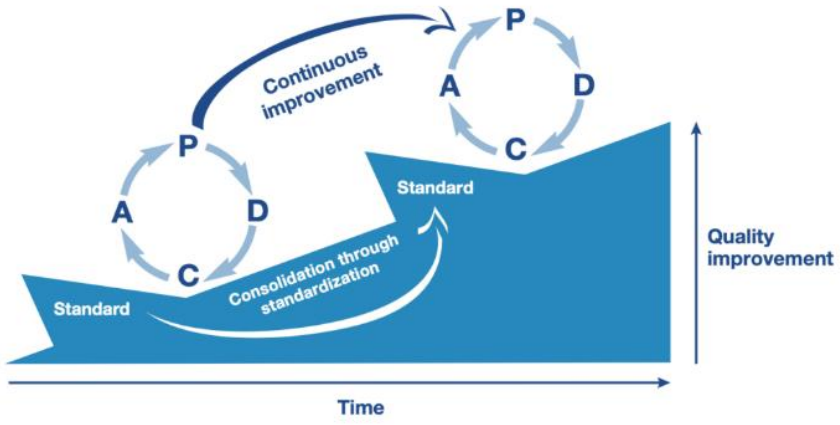
Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

4 RIADENIE BEZPEČNOSTI SYSTÉMOV AI V PROSTREDÍ ITVS PODĽA PDCA MODELU

V rámci tejto kapitoly sa zameriavame na ZoITVS a možnosti doplnenia bezpečnostných požiadaviek na správcov informačných technológií verejnej správy, pričom osobitná pozornosť je venovaná riadeniu bezpečnosti systémov AI. Kapitola identifikuje a systematizuje bezpečnostné opatrenia aplikovateľné na AI systémy v prostredí verejnej správy so zohľadnením ich špecifických rizík a charakteristík. Súčasťou sú aj praktické príklady implementácie týchto opatrení prostredníctvom prípadových štúdií, ktoré ilustrujú reálne scenáre využitia AI. Zároveň obsahuje návrhy vzorovej dokumentácie, ktorá môže slúžiť ako metodická podpora pre správcov ITVS pri zavádzaní a riadení bezpečnosti AI systémov. Analytický prístup kapitoly je založený na mapovaní bezpečnostných požiadaviek vyplývajúcich zo ZoITVS na jednotlivé fázy PDCA cyklu (Plan–Do–Check–Act) a ich následnom prepojení s požiadavkami normy ISO/IEC 42001:2023 pre riadenie systémov AI.

4.1 PDCA CYKLUS

PDCA (PLAN-DO-CHECK-ACT) cyklus je štvorfázový iteratívny proces, obvykle využívaný na zlepšenie a skvalitnenie obchodnej stratégie (Obr. č. 1). Spočiatku sa začína v malom meradle, kedy sa testujú prvotné účinky na procesy, pričom v závere je konečným cieľom celkové zlepšenie. Testovať sa môžu rôzne hypotézy, pričom pri ich potvrdení, alebo vyvrátení sú pri opakovanom vykonaní cyklu dostupné nové poznatky o skúmanom systéme. S rozšírenou znalosťou sa môžeme rozhodnúť vylepšiť, alebo pozmeniť cieľ a priblížiť sa k nemu každým ďalším cyklom. Otázkou však ostáva rýchlosť zlepšovania sa, čo hrá primárnu rolu v súvislosti s konkurenčným faktorom v dnešnom svete.



Obrázok č. 1: PDCA cyklus (prevzaté z[1]).

V nasledujúcich bodoch si podrobnejšie priblížime každú zo štyroch fáz tohto cyklu.

[1] https://www.lean.org/lexicon-terms/pdca/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Fáza PLAN predstavuje základ pre riadenie bezpečnosti informačných technológií verejnej správy. Zahŕňa definovanie cieľov, rozsahu a organizácie bezpečnosti, ako aj identifikáciu aktív a rizík. V tejto fáze sa vytvára bezpečnostná stratégia, politiky a dokumentácia. Kľúčové je určenie zodpovedností a zdrojov potrebných na implementáciu bezpečnostných opatrení. Výsledkom je systematický rámec pre riadenie informačnej bezpečnosti (ISMS). Nakoľko sa v tejto fáze zameriavame na očakávaný výstup, ktorý má byť v súlade so stanovenými cieľmi a postupmi, súčasťou zlepšenia je aj úplnosť a presnosť špecifikácie.

Fáza DO zahŕňa implementáciu navrhnutých bezpečnostných opatrení do praxe. Ide o vývoj, obstarávanie, nasadenie a prevádzku informačných systémov. Pri zavádzaní nových procesov je dobrou praxou ich otestovanie v obmedzenom rozsahu, kedy je možné pozrieť sa na prípadné efekty. Dôležitá je spolupráca s dodávateľmi a zabezpečenie bezpečného vývoja. Súčasťou je aj riadenie prevádzky, konfigurácie a incidentov. Cieľom je zabezpečiť reálnu ochranu systémov a údajov.

Fáza CHECK je zameraná na overovanie účinnosti bezpečnostných opatrení. Zahŕňa monitoring, audit a pravidelné hodnotenie bezpečnosti. Identifikujú sa nedostatky a zraniteľnosti. Výsledky slúžia ako vstup pre zlepšovanie systému, kedy sa porovnajú získané výsledky s očakávanými. Potom sa pozerá na možné rozdiely, čím vieme identifikovať trendy. Ide o kontinuálnu kontrolnú činnosť.

Fáza ACT predstavuje prijímanie nápravných a preventívnych opatrení. Vychádza z výsledkov monitorovania a auditov. Zahŕňa riešenie incidentov a aktualizáciu bezpečnostných opatrení. Cieľom je neustále zlepšovanie úrovne bezpečnosti, kedy sa analyzujú rozdiely a pozerá sa na ich príčiny. Ak nenastáva zlepšenie pri prechode týmito krokmi, je potrebné upraviť rozsah, v ktorom sa PDCA cyklus aplikuje, kým nedochádza k zlepšeniu plánu. Táto fáza uzatvára cyklus a zároveň iniciuje nové plánovanie.

4.2 PRÍKLADY BEZPEČNOSTNÝCH HROZIEB

V tejto kapitole bližšie popisujeme bezpečnostné hrozby, ktoré ohrozujú systémy AI. Vychádzame z nasledujúcich dokumentov:

- MITRE ATLAS[2],
- NIST AI Adversarial Machine Learning (AML) taxonómia[3],
- OWASP OWASP ML / LLM Top 10[4].

1. Data poisoning

Útočník zámerne vloží škodlivé alebo skreslené dáta do tréningového alebo dolaďovacieho datasetu, čím ovplyvní správanie modelu. Dôsledkom môže byť zníženie presnosti alebo systematické skreslenie výstupov. Príkladom je kompromitovaný dataset pre detekciu podvodov, ktorý naučí model ignorovať

[2] MITRE. (n.d.). *MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems*. Retrieved from https://atlas.mitre.org/

[3] National Institute of Standards and Technology. (2023). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations* (NIST AI 100-2e2023). https://doi.org/10.6028/NIST.AI.100-2e2023

[4] OWASP Foundation. (2023). *OWASP Top 10 for Large Language Model Applications*. Retrieved from https://owasp.org/www-project-top-10-for-large-language-model-applications/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

určitý typ podozrivých transakcií. Táto bezpečnostná hrozba patrí do taxonómií MITRE ATLAS a NIST AML taxonómie.

2. Evasion attack

Útočník manipuluje vstup tak, aby model pri inferencii urobil nesprávny záver bez zmeny samotného modelu. V praxi môže ísť o transakciu upravenú tak, aby vyzerala legitímne, hoci je podvodná. Ide o kľúčovú bezpečnostnú hrozbu najmä pri klasifikačných modeloch a detekčných systémoch.

3. Prompt injection

Pri generatívnych systémoch útočník vloží inštrukcie, ktoré obídu systémové pravidlá, zmenia správanie modelu alebo prinútia model vyzradiť interný kontext. Typickým príkladom je dokument alebo webstránka v RAG pipeline, ktorá obsahuje skrytý pokyn typu „ignoruj predchádzajúce pravidlá“. OWASP ML / LLM Top 10 ju uvádza ako najvýznamnejšiu pre aplikácie využívajúce veľké jazykové modely (LLM).

4. Model tampering / backdoor insertion

Útočník modifikuje model, checkpoint alebo parametre tak, aby sa za určitých podmienok správal škodlivo. Napríklad model funguje štandardne, ale pri špecifickom tokene alebo vzore vykoná nežiaduce správanie. Táto hrozba je kritická tam, kde sa používajú cudzie modely alebo neoverené checkpointy.

5. Model extraction

Útočník opakovaným dopytovaním API aproximuje chránený model a získa jeho funkcionalitu alebo obchodné know-how. Pri verejne dostupných endpointoch môže ísť o systematické zbieranie vstupov a výstupov s cieľom rekonštrukcie modelu. Sprievodca ho výslovne uvádza medzi bežnými AI hrozbami.

6. Supply-chain attack

Zraniteľnosť alebo kompromitácia môže byť zavlečená cez externý model, dataset, knižnicu, kontajner alebo embedding model. Pri AI je supply chain širší než v klasickom softvéri, lebo zahŕňa aj datasety, model cards a model registry.

7. Halucinácia

Halucinácia nie je len kvalitatívna chyba, ale aj bezpečnostný problém, ak systém generuje nepravdivé právne, technické alebo procedurálne informácie. V prostredí verejnej správy môže spôsobiť chybnú radu občanovi, nesprávny pracovný postup alebo reputačné a právne dôsledky.

8. Nedostatočný human oversight

Ak výstup zo systému AI nie je možné zmysluplne skontrolovať, spochybniť alebo zrušiť, organizácia stráca kontrolu nad rozhodovaním. To je kritické najmä tam, kde systémy AI ovplyvňujú osoby, ich práva alebo prístup k službám.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

4.3 KLASIFIKÁCIA SYSTÉMOV PODĽA AI AKTU

Klasifikácia rizika systémov AI podľa AI Aktu určuje, ktoré povinnosti súladu sa vzťahujú na systémy AI, pričom priamo ovplyvňuje prístup na trh a potenciálne sankcie až do výšky 35 miliónov eur alebo 7 % celosvetového obratu[5]. K bližšiemu pochopeniu bezpečnosti systémov AI a tiež k definovaniu prípadových štúdií uvádzame štyri kategórie systémov AI:

- zakázané praktiky využívajúce AI,
- vysokorizikové systémy AI,
- systémy AI s obmedzeným rizikom,
- systémy AI s minimálnym rizikom.

Zakázané praktiky využívajúce AI (neakceptovateľné riziko) - kategória zakázaných praktík využívajúcich AI podľa AI Aktu zahŕňa systémy, ktoré predstavujú neprijateľné riziko pre základné práva a hodnoty spoločnosti. Ide najmä o systémy, ktoré manipulujú správanie jednotlivcov, využívajú zraniteľnosť osôb alebo umožňujú plošné sledovanie bez primeraného právneho základu. Typickým znakom je zásah do autonómie jednotlivca alebo diskriminačný dopad. Regulácia v tomto prípade zavádza úplný zákaz používania takýchto systémov. Príklady systémov AI spadajúcich do tejto kategórie:

- sociálne skórovanie občanov verejnou správou,
- AI manipulácia správania detí v online hrách,
- real-time biometrická identifikácia vo verejnom priestore bez právneho základu,
- emóciami riadený nábor zamestnancov.

Vysokorizikové systémy AI (vysokorizikové systémy AI) sú definované ako systémy, ktoré majú významný dopad na bezpečnosť alebo základné práva jednotlivcov. Podľa AI Aktu podliehajú prísnym požiadavkám na riadenie rizík, kvalitu dát, transparentnosť a dohľad človeka. Typicky sa používajú v regulovaných oblastiach ako zdravotníctvo, doprava, verejná správa alebo zamestnanosť. Charakteristickým znakom je, že ovplyvňujú rozhodovanie o jednotlivcoch (napr. prístup k službám alebo právam). Tieto systémy nie sú zakázané, ale musia spĺňať rozsiahle compliance požiadavky. Nedodržanie týchto požiadaviek môže viesť k zákazu uvedenia na trh. Príklady systémov AI spadajúcich do tejto kategórie:

- systémy AI na hodnotenie úverovej bonity,
- systémy AI pre triedenie uchádzačov o zamestnanie,

[5] GDPRLocal. (2025, 3. november). *AI risk classification: Guide to EU AI Act risk categories*. https://gdprlocal.com/ai-risk-classification/

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- diagnostický systém AI v zdravotníctve.

Systémy AI s obmedzeným rizikom (limitované riziko) - predstavujú kategóriu, kde riziko pre základné práva je nižšie, ale stále vyžaduje určitú mieru transparentnosti. Podľa AI Aktu musia tieto systémy informovať používateľa o tom, že komunikuje s AI. Typickým príkladom sú chatboty alebo generatívne systémy. Regulácia nevyžaduje rozsiahle compliance opatrenia, ale kladie dôraz na informovanosť. Používatelia musia mať možnosť rozpoznať, že ide o systém AI. Cieľom je zabrániť klamaniu alebo nevedomému ovplyvňovaniu. Príklady systémov AI spadajúcich do tejto kategórie:

- chatbot verejnej správy,
- AI nástroj na sumarizáciu dokumentov,
- generatívny AI nástroj na tvorbu textov.

Systémy AI s minimálnym rizikom (minimálne riziko) - predstavujú najväčšiu skupinu systémov, ktoré nemajú významný dopad na základné práva ani bezpečnosť. Podľa AI Aktu nie sú predmetom špecifických regulačných požiadaviek. Ide o bežné systémy (aplikácie) AI používané v každodennom živote. Regulácia ich používanie neobmedzuje, ale odporúča dobrovoľné dodržiavanie etických princípov. Charakteristické je, že neovplyvňujú rozhodovanie o jednotlivcoch zásadným spôsobom. Riziko zneužitia je nízke. Príklady systémov AI spadajúcich do tejto kategórie:

- AI automatická korekcia textu,
- AI nástroj na úpravu fotografií,
- systém AI na optimalizáciu spotreby energie.

4.4 PRÍPADOVÉ ŠTÚDIE SYSTÉMOV AI

Pre lepšiu ilustráciu použitia systémov AI v rámci tohto materiálu sme navrhli tri prípadové štúdie, ktoré zahŕňajú systémy AI rôzneho typu, architektúry a účelu:

- AI nástroj na úpravu fotografií,
- AI chatbot pre komunikáciu s občanmi,
- systém AI pre triedenie uchádzačov o zamestnanie.

V rámci nasledujúcich podkapitol bližšie popisujeme jednotlivé prípadové štúdie. Pri každej prípadovej štúdii uvádzame architektúru systému podľa **Secure AI Framework (SAIF)** od spoločnosti Google. SAIF rozdeľuje systémy AI do štyroch komponentov[6]:

[6] Google. (n.d.). *Components of generative AI systems*. Secure AI Framework (SAIF). https://saif.google/secure-ai-framework/components

- **dáta** - vstupy používateľa spúšťajú statický kód, ktorý určuje logiku vedúcu k výsledkom programu. V prípade vývoja AI preberajú dáta úlohu, ktorú predtým plnil kód, čo zásadne mení charakter bezpečnostných a súkromnostných rizík.
- **infraštruktúra** – dátový komponent od infraštruktúry, ktorá ich podporuje, vrátane bezpečného hardvéru, odolného kódu, úložiska dát a platforiem pre vývoj a nasadenie. Riziká v tejto infraštruktúre môžu ovplyvniť kód modelu a frameworku, úložisko modelov a dát, ako aj samotné poskytovanie modelu (model serving).
- **model** - cieľom je aplikovať štatistické vzory extrahované z tréningových dát a využívať ich na generovanie nového textu, obrázkov, videí alebo iných výstupných dát (tzv. inferencií) na základe vstupných dát.
- **aplikácia** - niektoré AI modely reagujú na prirodzene formulované požiadavky používateľa, pričom výber slov a formulácia priamo ovplyvňujú spôsob, akým napríklad LLM interpretuje požiadavky, akcie a zámer. V porovnaní s interakciou prostredníctvom API táto priama interakcia vytvára nové vektory rizík, ako je napríklad prompt injection.

Súčasne v popise prípadových štúdií využívame klasifikáciu systémov AI podľa AI aktu a prípadovú štúdiu dopĺňame o príklady bezpečnostných hrozieb, ktoré sa jej dotýkajú. Klasifikáciu systémov AI podľa AI Aktu ako aj bezpečnostné hrozby sme bližšie popísali v predchádzajúcich kapitolách.

4.4.1 AI NÁSTROJ NA ÚPRAVU FOTOGRAFIÍ

Prvým príkladom je AI nástroj na úpravu fotografií, ktorý slúži na automatické zlepšovanie kvality obrazového materiálu, napr. zvýšenie rozlíšenia, odstránenie šumu alebo optimalizáciu farieb. V prostredí verejnej správy môže byť využívaný napríklad na spracovanie dokumentov, digitalizáciu archívov alebo publikovanie vizuálneho obsahu na webových portáloch. Systém využíva modely počítačového videnia (napr. CNN alebo diffusion-based modely) na transformáciu vstupných obrázkov. Nevykonáva rozhodovanie o právach alebo povinnostiach osôb a jeho výstupy majú čisto podporný charakter. Spracovanie dát je obmedzené na obrazové vstupy bez potreby identifikácie osôb. Použitie je bežné aj v komerčných nástrojoch na úpravu fotografií.

Architektúra systému:

- **Dáta:** obrázky (napr. skeny dokumentov, fotografie), prípadne verejné dataset-y pre tréning modelu.
- **Model:** modely počítačového videnia (napr. super-resolution CNN, diffusion modely).
- **Infraštruktúra:** cloud alebo lokálne nasadenie (on-prem), bez potreby citlivých integrácií.
- **Aplikácia:** desktop aplikácia, webový nástroj alebo API pre spracovanie obrázkov.

Klasifikácia podľa AI Aktu:

Systém spadá do kategórie **minimálne riziko**, keďže neovplyvňuje práva, povinnosti ani bezpečnosť jednotlivcov. Ide o pomocný nástroj bez rozhodovacej funkcie. Povinnosti podľa AI Aktu sú minimálne,

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

pričom sa odporúča dodržiavať základné princípy kvality a bezpečnosti. Transparentnosť alebo auditovateľnosť nie sú striktne vyžadované.

Príklady bezpečnostných hrozieb:

- manipulácia obrazového obsahu (napr. neúmyselná zmena významu vizuálneho dôkazu),
- data poisoning pri tréningu modelu (ovplyvnenie kvality výstupov),
- nesprávna interpretácia upravených obrázkov používateľom.

4.4.2 AI CHATBOT PRE KOMUNIKÁCIU S OBČANMI

Druhým príkladom je AI chatbot, ktorý je nasadený vo verejnej správe na automatizovanú komunikáciu s občanmi pri vybavovaní agendy (dane, sociálne dávky, stavebné konania). Systém využíva veľký jazykový model (LLM) na spracovanie prirodzeného jazyka a generovanie odpovedí na základe interných smerníc a verejných dokumentov. Systém AI pracuje s potenciálne citlivými údajmi (napr. identifikácia občana), čo zvyšuje požiadavky na bezpečnosť a ochranu osobných údajov. Interakcia prebieha cez webový prehliadač alebo mobilnú aplikáciu. Výstupy systému majú informatívny charakter, ale môžu ovplyvniť rozhodovanie používateľa.

Architektúra systému:

- **Dáta:** legislatívne dokumenty, interné smernice, open data portály, FAQ databázy, používateľské vstupy.
- **Model:** LLM s RAG komponentom pre dotazovanie znalostnej bázy.
- **Infraštruktúra:** hybrid (cloud pre model, on-prem pre citlivé registre), API integrácie na eGovernment služby.
- **Aplikácia:** webový chatbot, mobilná aplikácia, API rozhranie pre ďalšie systémy.

Klasifikácia podľa AI aktu:

Systém spadá do kategórie **limitované riziko**, keďže ide o interakciu s používateľom prostredníctvom AI (chatbot), pričom je potrebná transparentnosť (informovanie, že ide o systém AI). V prípade prepojenia na rozhodovacie procesy alebo personalizované odporúčania môže prejsť do **vysokého rizika** (napr. ak ovplyvňuje prístup k verejným službám).

Príklady bezpečnostných hrozieb:

- prompt injection (manipulácia odpovedí cez vstupy používateľa),
- leakage citlivých údajov (napr. z kontextu alebo tréningových dát),

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- model hallucination vedúci k nesprávnym informáciám.

4.4.3 SYSTÉM AI PRE TRIEDENIE UCHÁDZAČOV O ZAMESTNANIE

Poslednou prípadovou štúdiou je systém AI pre triedenie uchádzačov o zamestnanie, ktorý je nasadený v organizáciách verejnej správy alebo regulovaného sektora na automatizované predvýberové hodnotenie kandidátov na základe životopisov, motivačných listov a ďalších údajov. Systém využíva techniky spracovania prirodzeného jazyka (NLP) a strojového učenia na identifikáciu relevantných kvalifikácií, skúseností a zhody s požiadavkami pracovnej pozície. V praxi reflektuje existujúce HR nástroje používané na optimalizáciu náborového procesu a zníženie administratívnej záťaže. Výstupy systému majú priamy dopad na to, ktorí kandidáti postúpia do ďalších fáz výberového konania. Systém pracuje s osobnými údajmi, čo vyžaduje súlad s ochranou osobných údajov a zásadami spravodlivého spracovania. Rozhodovanie môže byť plne automatizované alebo podporované ľudským dohľadom.

Architektúra systému:

- **Dáta:** životopisy, motivačné listy, HR databázy, historické dáta o prijatých kandidátoch.
- **Model:** NLP modely (klasifikácia, ranking), prípadne hybridné modely s pravidlami.
- **Infraštruktúra:** cloud alebo hybridné riešenie, integrácia s HR systémami (ATS).
- **Aplikácia:** HR dashboard, automatizovaný screening nástroj, API pre náborové platformy.

Klasifikácia podľa AI Aktu:

Systém je klasifikovaný ako **vysoké riziko**, keďže sa používa v oblasti zamestnania a má významný dopad na prístup jednotlivcov k pracovným príležitostiam. AI Akt explicitne zaraďuje systémy pre nábor a výber zamestnancov medzi vysokorizikové. Povinnosti zahŕňajú zavedenie risk management systému, zabezpečenie kvality a reprezentatívnosti dát, transparentnosť, vysvetliteľnosť rozhodnutí, auditovateľnosť a zabezpečenie ľudského dohľadu. Dôležité je aj minimalizovanie diskriminácie a biasu.

Príklady bezpečnostných hrozieb:

- bias a diskriminácia (napr. na základe pohlavia, veku alebo pôvodu),
- data poisoning (ovplyvnenie tréningových dát s cieľom manipulovať výstupy),
- nesprávne rozhodnutia (false positives / negatives pri výbere kandidátov).

4.5 PLÁNOVANIE BEZPEČNOSTI SYSTÉMOV AI (FÁZA PLAN)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Medzi bezpečnostné opatrenia, ktoré musia plniť správcovia ITVS vo fáze **PLAN**, patria najmä ustanovenia § 18 a § 19 ZoITVS. Ustanovenie § 18 definuje základnú povinnosť správcu prijímať a realizovať bezpečnostné opatrenia v závislosti od klasifikácie informácií a kategorizácie systémov, pričom umožňuje aj uplatnenie prísnejších opatrení. Ustanovenie § 19 ods. 1 písm. a) vytvára rámec riadenia bezpečnosti prostredníctvom definovania cieľov, rozsahu, podmienok a procesov, pričom zahŕňa aj organizačné zabezpečenie, riadenie aktív a rizík, implementáciu opatrení, zabezpečenie zdrojov, kontrolu a postupy riešenia incidentov (§ 19 ods. 1 písm. b) až g)). Ustanovenie § 19 ods. 2 upravuje schvaľovanie opatrení vyplývajúcich z incidentov, analýz, auditov a kontrol, čím zabezpečuje spätnú väzbu do riadenia bezpečnosti. Ustanovenie § 19 ods. 5 dopĺňa plánovaciu fázu o strategické prvky, ako je dodržiavanie bezpečnostnej stratégie, určenie zodpovednej osoby a identifikácia rizík prostredia. Do tejto fázy zároveň patria aj ustanovenia § 23, ktoré zahŕňajú identifikáciu kritických systémov, evidenciu aktív, reporting a pravidlá pre oznamovanie zraniteľností.

Správca ITVS musí v rámci plánovania bezpečnosti AI systémov zabezpečiť vytvorenie a zdokumentovanie AI politiky, jasné priradenie rolí a zodpovedností a identifikáciu všetkých relevantných zdrojov naprieč životným cyklom systému. Zároveň musí definovať procesy pre zodpovedný návrh, vývoj, overovanie a validáciu AI systémov, vrátane mechanizmov komunikácie incidentov a zosúladenia s existujúcimi organizačnými politikami. Nevyhnutnou súčasťou je aj zavedenie procesu posudzovania dopadov AI na jednotlivcov a spoločnosť, ako aj mechanizmov na oznamovanie obáv a transparentnú komunikáciu so zainteresovanými stranami. Správca musí tiež zabezpečiť jasné rozdelenie zodpovedností medzi všetky zapojené subjekty v rámci životného cyklu AI systému.

V nasledujúcej kapitole uvádzame zoznam (checklist) jednotlivých bezpečnostných opatrení pre AI systémy vo fáze plánovania s odkazom na prislúchajúcu časť normy ISO/EIC 42001:2023). **V prílohe A** je uvedené úplné mapovanie jednotlivých ustanovení ZoITVS k norme ISO/EIC 42001:2023.

4.5.1 BEZPEČNOSTNÉ OPATRENIA

Správca informačných technológií verejnej správy by mal vykonať nasledujúce bezpečnostné opatrenia:

- zdokumentovať politiku pre vývoj alebo používanie systémov AI (ISO/IEC 42001:2023 – A.2.2 AI policy),
- definovať a prideliť úlohy a zodpovednosti pre AI podľa potrieb organizácie (ISO/IEC 42001:2023 – A.3.2 AI roles and responsibilities),
- identifikovať a dokumentovať relevantné zdroje potrebné pre činnosti v daných fázach životného cyklu systému AI a ďalšie činnosti súvisiace s AI, ktoré sú pre organizáciu relevantné (ISO/IEC 42001:2023 – A.4.2 Resource documentation),
- definovať a dokumentovať konkrétne procesy pre zodpovedný návrh a vývoj systému AI (ISO/IEC 42001:2023 – A.6.1.3 Processes for responsible AI system design and development),
- identifikovať a dokumentovať relevantné zdroje potrebné pre činnosti v daných fázach životného cyklu systému AI a ďalšie činnosti súvisiace s AI, ktoré sú pre organizáciu relevantné (ISO/IEC 42001:2023 – A.4.2 Resource documentation),

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- definovať a dokumentovať opatrenia overovania a validácie pre systém AI a špecifikovať kritériá ich použitia (ISO/IEC 42001:2023 – A.6.2.4 AI system verification and validation),
- určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI (ISO/IEC 42001:2023 – A.8.4 Communication of incidents),
- určiť, kde môžu byť iné organizačné politiky ovplyvnené cieľmi organizácie vo vzťahu k systémom AI alebo kde sa na ne tieto ciele uplatňujú (ISO/IEC 42001:2023 – A.2.3 Alignment with other organizational policies),
- definovať a prideliť úlohy a zodpovednosti pre AI podľa potrieb organizácie (ISO/IEC 42001:2023 – A.3.2 AI roles and responsibilities),
- zaviesť proces na posudzovanie možných dôsledkov pre jednotlivcov alebo skupiny jednotlivcov, alebo pre oboje, a spoločnosti, ktoré môžu vyplynúť zo systému AI počas celého jeho životného cyklu (ISO/IEC 42001:2023 – A.5.2 AI system impact assessment process),
- identifikovať a dokumentovať relevantné zdroje potrebné pre činnosti v daných fázach životného cyklu systému AI a ďalšie činnosti súvisiace s AI, ktoré sú pre organizáciu relevantné (ISO/IEC 42001:2023 – A.4.2 Resource documentation),
- definovať a zaviesť proces na oznamovanie obáv týkajúcich sa úlohy organizácie vo vzťahu k systému AI počas celého jeho životného cyklu (ISO/IEC 42001:2023:2023 – A.3.3 Reporting of concerns),
- zabezpečiť, aby boli zodpovednosti v rámci životného cyklu systému AI rozdelené medzi organizáciu, jej partnerov, dodávateľov, zákazníkov a tretie strany (ISO/IEC 42001:2023 – A.10.2 Allocating responsibilities),
- určiť a zdokumentovať svoje povinnosti týkajúce sa oznamovania informácií o systéme AI zainteresovaným stranám (ISO/IEC 42001:2023 – A.8.5 Information for interested parties).

4.5.2 PRÍPADOVÉ ŠTÚDIE

AI nástroj na úpravu fotografií

Správca ITVS musí zdokumentovať politiku používania AI nástroja na úpravu fotografií so zameraním na zachovanie integrity obrazových dát, najmä pri spracovaní archívnych alebo dôkazových materiálov (A.2.2). Musí definovať zodpovednosti medzi IT administrátormi a používateľmi systému, napr. kto schvaľuje použitie nástroja na oficiálne dokumenty (A.3.2, A.10.2). V rámci AI impact assessment musí posúdiť riziko zmeny významu obrazového obsahu, napr. pri digitalizácii dokumentov (A.5.2). Musí tiež zaviesť mechanizmus na nahlasovanie problémov, napr. nesprávne upravených obrázkov používateľmi (A.3.3).

AI chatbot pre komunikáciu s občanmi

Správca ITVS musí zdokumentovať politiku používania chatbotu tak, aby bolo výslovne určené, že ide o nástroj s informatívnou funkciou, nie o autonómny rozhodovací systém, a aby politika pokrývala transparentnosť voči občanovi, ochranu osobných údajov a limity použitia modelu (A.2.2, A.2.3). Správca ITVS musí jasne definovať zodpovednosti medzi prevádzkovateľom systému, dodávateľom

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

LLM a správcom údajov (A.3.2, A.10.2). V rámci návrhu musí identifikovať zdroje dát (legislatíva, registre, vstupy používateľa) a vyhodnotiť ich kvalitu a riziká úniku (A.4.2, A.5.2). Súčasne musí definovať procesy návrhu RAG architektúry s dôrazom na bezpečné dotazovanie znalostnej bázy a ochranu pred prompt injection (A.6.1.3). Organizácia musí stanoviť pravidlá validácie odpovedí chatbotu a plán komunikácie incidentov, napr. pri úniku údajov alebo nesprávnych odpovediach (A.6.2.4, A.8.4).

Systém AI pre triedenie uchádzačov o zamestnanie

Organizácia musí zdokumentovať AI politiku pre HR screening systém vrátane pravidiel na prevenciu diskriminácie a zabezpečenie férovosti výberu kandidátov (A.2.2). Musí definovať zodpovednosti medzi HR oddelením, IT a dodávateľom AI modelu, napr. kto schvaľuje modelové zmeny a kto vykonáva audit biasu (A.3.2, A.10.2). V rámci AI impact assessment musí analyzovať dopady na práva uchádzačov, napr. riziko diskriminácie na základe historických dát (A.5.2). Musí tiež zaviesť mechanizmus na nahlasovanie obáv kandidátov, napr. možnosť odvolania proti rozhodnutiu AI (A.3.3).

4.5.3 PRÍKLAD DOKUMENTÁCIE

Pre plánovanie bezpečnosti AI systémov (fáza PLAN) môže správca informačných technológií verejnej správy prijať nasledujúce riadiace dokumenty:

- **Politika AI a bezpečnosti AIMS (manažment systému AI)** - definuje základné princípy, smerovanie a záväzky organizácie pri riadení systémov AI systémov vrátane bezpečnosti, etiky a súladu. Slúži ako rámec pre stanovenie cieľov AIMS a rozhodovanie manažmentu. Väzba na ISO/IEC 42001:2023 - A.2.2, A.2.3.
- **Organizačná štruktúra AIMS (roly a zodpovednosti)** - určuje zodpovednosti, právomoci a kompetencie jednotlivých rolí v rámci životného cyklu AI. Zabezpečuje oddelenie riadiacich, výkonných a kontrolných funkcií. Väzba na ISO/IEC 42001:2023 - A.3.2.
- **Katalóg aktív AI a ITVS** - eviduje všetky relevantné aktíva vrátane AI modelov, dát, infraštruktúry a nástrojov. Slúži ako vstup pre riadenie rizík a analýzu dopadov. Väzba na ISO/IEC 42001:2023 - A.4.2–A.4.5.
- **Metodika riadenia rizík AI** – definuje proces identifikácie, analýzy a ošetrenia rizík AI vrátane kritérií prijateľnosti rizika. Umožňuje systematické riadenie rizík počas celého životného cyklu AI. Väzba na ISO/IEC 42001:2023 - kap. 6.1.2–6.1.3.
- **AI Impact Assessment (AIIA)** – formalizovaný proces hodnotenia dopadov AI na jednotlivcov, skupiny a spoločnosť. Výsledky sa využívajú pri rozhodovaní o nasadení a mitigácii rizík. Väzba na ISO/IEC 42001:2023 - A.5.2–A.5.5.
- **Bezpečnostná stratégia AI/ITVS** – definuje strategické ciele a smerovanie bezpečnosti AI v súlade s organizáciou a legislatívou. Prepája AI riadenie s ostatnými politikami (napr. kybernetická bezpečnosť). Väzba na ISO/IEC 42001:2023 - A.2.3.
- **Plán zdrojov AIMS** – identifikuje potrebné ľudské, technické a dátové zdroje pre fungovanie AIMS. Zabezpečuje, že organizácia má dostatočné kapacity na riadenie AI. Väzba na ISO/IEC 42001:2023 - A.4.2–A.4.6.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- **Plán riadenia incidentov AI** – definuje postupy detekcie, eskalácie a riešenia incidentov súvisiacich s AI. Obsahuje aj pravidlá komunikácie so zainteresovanými stranami. Väzba na ISO/IEC 42001:2023 - A.8.4.
- **Klasifikácia a kritickosť systémov AI** – určuje úroveň kritickosti systémov AI na základe dopadov a rizík. Slúži na prioritizáciu bezpečnostných opatrení a kontrol. Väzba na ISO/IEC 42001:2023 - A.5.2.

4.6 Implementácia a prevádzka systémov AI (fáza DO)

Do fázy **DO** patria najmä ustanovenia § 20 a § 21 zákona o ITVS. Ustanovenie § 20 ods. 1 stanovuje povinnosť určiť bezpečnostné požiadavky na informačný systém verejnej správy vrátane podmienok jeho vývoja, testovania a dodania, ako aj zabezpečiť vypracovanie bezpečnostnej dokumentácie vrátane bezpečnostného projektu. Ustanovenie § 20 ods. 2 upravuje požiadavky na bezpečné vývojové prostredie, dokumentáciu vývoja a testovania, povinnosť mlčanlivosti dodávateľa a odstránenie funkcií umožňujúcich neoprávnený prístup do systému. Ustanovenie § 21 upravuje zavedenie, prevádzku a vyradenie ISVS, pričom pred uvedením do prevádzky je potrebné overiť splnenie bezpečnostných požiadaviek a vykonať bezpečnostné testovanie pre systémy spracúvajúce citlivé údaje. Ustanovenia § 23 zároveň dopĺňajú túto fázu o prijímanie bezpečnostných opatrení na základe testovania, hodnotenia zraniteľností a incidentov, ako aj o povinnosti súvisiace s ich hlásením.

Správca ITVS musí v rámci implementácie a prevádzky systémov AI zabezpečiť špecifikáciu a dokumentáciu požiadaviek na AI systémy, ako aj riadený návrh a vývoj v súlade s organizačnými cieľmi a kritériami. Súčasne musí definovať procesy pre zodpovedný vývoj, vrátane overovania a validácie systémov s jasne stanovenými kritériami kvality. Pred nasadením je povinný zdokumentovať plán nasadenia a zabezpečiť splnenie všetkých požiadaviek, ako aj pripraviť podmienky pre bezpečnú a kontinuálnu prevádzku systému. Nevyhnutnou súčasťou je aj zavedenie mechanizmov na komunikáciu incidentov používateľom a riadenie prevádzkových udalostí.

V nasledujúcej kapitole uvádzame zoznam (checklist) jednotlivých bezpečnostných opatrení pre AI systémy vo fáze plánovania s odkazom na prislúchajúcu časť normy ISO/EIC 42001:2023). **V prílohe B** je uvedené úplné mapovanie jednotlivých ustanovení ZoITVS k norme ISO/EIC 42001:2023.

4.6.1 Bezpečnostné opatrenia

Správca informačných technológií verejnej správy by mal vykonať nasledujúce bezpečnostné opatrenia:

- špecifikovať a dokumentovať požiadavky na nové systémy AI alebo podstatné vylepšenia existujúcich systémov (ISO/IEC 42001 – A.6.2.2 AI system requirements and specification),
- dokumentovať návrh a vývoj systému AI na základe organizačných cieľov, zdokumentovaných požiadaviek a kritérií špecifikácie. (ISO/IEC 42001 – A.6.2.3 Documentation of AI system design and development),
- definovať a dokumentovať konkrétne procesy pre zodpovedný návrh a vývoj systému AI (ISO/IEC 42001 – A.6.1.3 Processes for responsible AI system design and development)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- zdokumentovať plán nasadenia a zabezpečiť, aby boli pred nasadením splnené príslušné požiadavky (ISO/IEC 42001 – A.6.2.5 AI system deployment),
- zdokumentovať plán nasadenia a zabezpečiť, aby boli pred nasadením splnené príslušné požiadavky. Súčasne musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI (ISO/IEC 42001 – A.6.2.5 / A.6.2.6),
- definovať a dokumentovať opatrenia overovania a validácie pre systém AI a špecifikovať kritériá ich použitia (ISO/IEC 42001 – A.6.2.4 AI system verification and validation),
- určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI (ISO/IEC 42001 – A.8.4 Communication of incidents).

4.6.2 PRÍPADOVÉ ŠTÚDIE

AI nástroj na úpravu fotografií

Správca ITVS musí špecifikovať požiadavky na AI systém, napr. že výstup nesmie meniť obsah dokumentu spôsobom, ktorý by ovplyvnil jeho interpretáciu (A.6.2.2). Pri návrhu systému musí dokumentovať použité modely (napr. super-resolution) a ich vplyv na kvalitu výstupov (A.6.2.3). Musí zaviesť validačné mechanizmy, napr. porovnanie vstupu a výstupu na detekciu nežiaducich zmien (A.6.2.4). Pred nasadením musí otestovať systém na reálnych datasetoch (napr. skeny dokumentov) a definovať postupy riešenia incidentov (A.6.2.5, A.8.4).

AI chatbot pre komunikáciu s občanmi

Organizácia musí špecifikovať požiadavky na chatbot vrátane bezpečnostných požiadaviek na spracovanie vstupov a ochranu pred manipuláciou promptov (A.6.2.2). Návrh systému musí byť zdokumentovaný vrátane architektúry RAG a integrácií na eGovernment API (A.6.2.3). Pri nasadení musí zabezpečiť, že systém neumožňuje prístup k citlivým údajom mimo autorizovaného kontextu (A.6.2.5). Musí zaviesť prevádzkové opatrenia ako monitoring odpovedí, logovanie interakcií a detekciu anomálií (A.6.2.6). Validácia musí zahŕňať testovanie hallucination a kvality odpovedí na reálnych scenároch (A.6.2.4).

Systém AI pre triedenie uchádzačov o zamestnanie

Musí špecifikovať požiadavky na AI systém tak, aby zahŕňali metriky férovosti (fairness metrics) a presnosti pri výbere kandidátov (A.6.2.2). Pri návrhu systému musí dokumentovať použité dátové zdroje a modelové rozhodovacie kritériá, napr. váhy atribútov v ranking modeli (A.6.2.3). Musí implementovať validačné mechanizmy na detekciu biasu, napr. testovanie modelu na rôznych demografických skupinách (A.6.2.4). Pred nasadením musí overiť, že systém neprodukuje systematicky diskriminačné výstupy a definovať postupy reakcie na incidenty (A.6.2.5, A.8.4).

4.6.3 PRÍKLAD DOKUMENTÁCIE

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Pre implementáciu a prevádzku bezpečnosti systémov AI (fáza DO) môže správca informačných technológií verejnej správy prijať nasledujúce riadiace dokumenty:

- **Špecifikácia systému AI** – popisuje funkčné, bezpečnostné a výkonnostné požiadavky na systém AI. Slúži ako základ pre návrh, vývoj a validáciu systému. Väzba na ISO/IEC 42001:2023 - A.6.2.2.
- **Bezpečnostný projekt systému AI** – komplexný návrh architektúry, bezpečnostných opatrení a kontrol pre systém AI. Zabezpečuje súlad medzi požiadavkami, rizikami a implementáciou. Väzba na ISO/IEC 42001:2023 - A.6.2.3.
- **Secure SDLC pre AI (proces vývoja)** – definuje bezpečný životný cyklus vývoja AI vrátane návrhu, tréningu, testovania a nasadenia. Zohľadňuje špecifiká AI ako bias, kvalita dát a model drift. Väzba na ISO/IEC 42001:2023 - A.6.1.3.
- **Plán nasadenia systému AI** – určuje podmienky, kroky a kontroly potrebné pred uvedením systému AI do prevádzky. Zabezpečuje, že všetky požiadavky sú splnené pred deploymentom. Väzba na ISO/IEC 42001:2023 - A.6.2.5.
- **Testovací plán (verifikácia a validácia)** – definuje metodiku testovania systému AI vrátane bezpečnostných, funkčných a výkonnostných testov. Umožňuje preukázať splnenie požiadaviek. Väzba na ISO/IEC 42001:2023 - A.6.2.4.
- **Prevádzková dokumentácia systému AI** – popisuje postupy prevádzky, údržby, monitorovania a podpory systému AI. Zabezpečuje stabilnú a bezpečnú prevádzku. Väzba na ISO/IEC 42001:2023 - A.6.2.6.
- **Bezpečnostné testovanie (penetračné testy)** – dokumentuje testovanie zraniteľností a odolnosti systému voči útokom. Slúži na identifikáciu a odstránenie slabín. Väzba na ISO/IEC 42001:2023 - A.6.2.4.
- **Zmluvy a požiadavky na dodávateľov systémov AI** – definuje bezpečnostné, etické a prevádzkové požiadavky na dodávateľov systémov AI. Zabezpečuje riadenie rizík tretích strán. Väzba na ISO/IEC 42001:2023 - A.10.2–A.10.3.
- **Politika a riadenie dát pre systémy AI** – upravuje získavanie, kvalitu, prípravu a správu dát používaných v systémoch AI. Minimalizuje riziká biasu a nekvalitných dát. Väzba na ISO/IEC 42001:2023 - A.7.2–A.7.6.

4.7 MONITOROVANIE A HODNOTENIE SYSTÉMOV AI (FÁZA CHECK)

Do **fázy CHECK** patria najmä ustanovenia § 21 ods. 3 písm. a) a písm. b) body 5 a 6, § 22, § 23 ods. 5 písm. a) a f) a § 23a ods. 2 písm. a), b) a c) zákona o ITVS. Ustanovenie § 21 ods. 3 upravuje zabezpečenie monitorovania informačných systémov, riadenie konfigurácie a vykonávanie kontrolných a auditných činností. Ustanovenie § 22 ustanovuje povinnosť pravidelného monitorovania, testovania a hodnotenia bezpečnosti informačných systémov podľa osobitného predpisu. Ustanovenia § 23 ods. 5 zavádzajú evidenciu incidentov a realizáciu bezpečnostných opatrení na základe ich vyhodnotenia. § 23a ods. 2 zároveň zahŕňa vykonávanie činností na riešenie bezpečnostných incidentov, prevenciu, ako aj hodnotenie zraniteľností. Táto fáza tak zabezpečuje systematické monitorovanie, kontrolu a spätnú väzbu pre priebežné riadenie bezpečnosti systémov AI.

Správca ITVS musí v rámci monitorovania a hodnotenia systémov AI zabezpečiť dostupnosť a poskytovanie primeranej technickej dokumentácie pre všetky relevantné zainteresované strany. Zároveň

musí definovať a realizovať procesy priebežnej prevádzky, ktoré zahŕňajú monitorovanie výkonnosti systému, jeho údržbu, aktualizácie a podporu. Nevyhnutnou súčasťou je aj zavedenie mechanizmov na komunikáciu incidentov a procesov pre zodpovedné používanie AI systémov. Súčasne musí umožniť efektívne oznamovanie obáv súvisiacich s fungovaním AI systému počas celého jeho životného cyklu.

V nasledujúcej kapitole uvádzame zoznam (checklist) jednotlivých bezpečnostných opatrení pre systémy AI vo fáze monitorovania a hodnotenie systémov AI s odkazom na prislúchajúcu časť normy ISO/EIC 42001:2023). **V prílohe C** je uvedené úplné mapovanie jednotlivých ustanovení ZoITVS k norme ISO/EIC 42001:2023.

4.7.1 BEZPEČNOSTNÉ OPATRENIA

Správca informačných technológií verejnej správy by mal vykonať nasledujúce bezpečnostné opatrenia:

- určiť, aká technická dokumentácia systému AI je potrebná pre každú relevantnú kategóriu zainteresovaných strán, ako sú používatelia, partneri, dozorné orgány a poskytnúť im technickú dokumentáciu vo vhodnej forme (ISO/IEC 42001:2023 – A.6.2.7 AI system technical documentation),
- definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu (ISO/IEC 42001:2023 – A.6.2.6 AI system operation and monitoring),
- určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI (ISO/IEC 42001:2023 – A.8.4 Communication of incidents),
- definovať a dokumentovať procesy pre zodpovedné používanie systémov AI (ISO/IEC 42001:2023 – A.9.2 Processes for responsible use of AI systems),
- definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu (ISO/IEC 42001:2023 – A.6.2.6 AI system operation and monitoring),
- definovať a zaviesť proces na oznamovanie obáv týkajúcich sa úlohy organizácie vo vzťahu k systému AI počas celého jeho životného cyklu (ISO/IEC 42001:2023 – A.3.3 Reporting of concerns).

4.7.2 PRÍPADOVÉ ŠTÚDIE

AI nástroj na úpravu fotografií

Správca ITVS musí zabezpečiť technickú dokumentáciu systému, napr. opis algoritmov a ich vplyvu na obrazové dáta pre používateľov a audítorov (A.6.2.7). Počas prevádzky musí monitorovať kvalitu výstupov, napr. identifikovať prípady degradácie obrazu alebo artefaktov (A.6.2.6). Musí definovať pravidlá používania systému, napr. zákaz použitia na forenzné dôkazy bez validácie (A.9.2). Musí tiež umožniť používateľom nahlasovať problémy s kvalitou výstupov (A.3.3).

AI chatbot pre komunikáciu s občanmi

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Organizácia musí zabezpečiť technickú dokumentáciu chatbotu pre rôzne skupiny (napr. administrátori, audítori, dozorné orgány) vrátane popisu modelu a dátových tokov (A.6.2.7). Prevádzka musí byť priebežne monitorovaná, najmä z pohľadu nesprávnych odpovedí a pokusov o prompt injection (A.6.2.6). Musí definovať pravidlá používania systému pre zamestnancov aj občanov, napr. obmedzenia použitia (A.9.2). Incidenty, ako únik dát alebo nesprávne odporúčania, musia byť dokumentované a komunikované (A.8.4). Organizácia musí zaviesť mechanizmy na nahlasovanie problémov (napr. feedback používateľov) (A.3.3).

Systém AI pre triedenie uchádzačov o zamestnanie

Musí zabezpečiť technickú dokumentáciu systému vrátane vysvetlenia rozhodovacích mechanizmov pre auditné orgány a HR používateľov (A.6.2.7). Počas prevádzky musí kontinuálne monitorovať výkonnosť modelu a identifikovať odchýlky, napr. zvýšený počet zamietnutých kandidátov z určitej skupiny (A.6.2.6). Musí definovať pravidlá používania AI, napr. zákaz plne automatizovaného rozhodovania bez ľudského zásahu (A.9.2). Súčasne musí umožniť nahlasovanie problémov zo strany HR alebo kandidátov (A.3.3).

4.7.3 PRÍKLAD DOKUMENTÁCIE

Pre monitorovanie a hodnotenie bezpečnosti AI systémov (fáza CHECK) môže správca informačných technológií verejnej správy prijať nasledujúce riadiace dokumenty:

- **Monitoring systémov AI** – definuje metriky, nástroje a procesy na sledovanie výkonu a bezpečnosti systémov AI. Umožňuje včas identifikovať odchýlky a incidenty. Väzba na ISO/IEC 42001:2023 - A.6.2.6.
- **Technická dokumentácia systému AI systému** – poskytuje detailný popis architektúry, modelov, dát a fungovania AI systému pre rôzne zainteresované strany. Zvyšuje transparentnosť a auditovateľnosť. Väzba na ISO/IEC 42001:2023 - A.6.2.7.
- **Interný audit AIMS** – definuje postupy pravidelného auditu systému riadenia AI a overovania súladu s normou. Slúži na identifikáciu nedostatkov. Väzba na ISO/IEC 42001:2023 - kap. 9.2.
- **Register incidentov AI** – eviduje všetky bezpečnostné incidenty, ich priebeh a riešenie. Umožňuje analýzu trendov a zlepšovanie bezpečnosti. Väzba na ISO/IEC 42001:2023 - A.8.4.
- **Hodnotenie zraniteľností systému AI systému** – pravidelné posudzovanie slabín systému a infraštruktúry. Podporuje preventívne riadenie rizík. Väzba na ISO/IEC 42001:2023 - A.6.2.6.
- **Reportovanie incidentov (napr. CSIRT)** – definuje procesy externého hlásenia incidentov a komunikácie s regulačnými orgánmi. Zabezpečuje súlad a transparentnosť. Väzba na ISO/IEC 42001:2023 - A.3.3, A.8.5.
- **Vyhodnotenie výkonnosti AI** – hodnotí efektívnosť systémov AI a AIMS na základe metrík. Podporuje rozhodovanie manažmentu. Väzba na ISO/IEC 42001:2023 - kap. 9.1.

4.8 ZLEPŠOVANIE SYSTÉMOV AI A REAKCIA NA INCIDENTY (FÁZA ACT)

Do **fázy ACT** patria najmä ustanovenia § 19 ods. 2 písm. b) a c), § 21 ods. 4, § 23 ods. 1 a § 23a ods. 1 písm. a) a ods. 2 písm. e) zákona o ITVS. Ustanovenie § 19 ods. 2 upravuje prijímanie a schvaľovanie

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

opatrení na základe závažných bezpečnostných incidentov, analýz, auditov a kontrol s cieľom minimalizovať ich opätovný výskyt. Ustanovenie § 23 ods. 1 definuje bezpečnostný projekt ako základný nástroj riadenia bezpečnosti, ktorý musí byť priebežne aktualizovaný, zatiaľ čo § 21 ods. 4 rieši bezpečné vyradenie informačných systémov z prevádzky ako súčasť životného cyklu. Ustanovenia § 23a zabezpečujú metodické usmerňovanie, zvyšovanie povedomia a vykonávanie činností na riešenie incidentov a hodnotenie zraniteľností. Fáza ACT tak predstavuje kontinuálne zlepšovanie bezpečnosti systémov AI na základe skúseností, analýz a identifikovaných rizík.

Správca ITVS musí v rámci zlepšovania systémov AI a reakcie na incidenty zabezpečiť zavedenie a pravidelnú aktualizáciu mechanizmov komunikácie incidentov používateľom. Zároveň musí priebežne preskúmavať AI politiku a aktualizovať ju tak, aby zostala účinná a v súlade s aktuálnymi požiadavkami a rizikami. Nevyhnutné je aj dokumentovanie kompetencií zapojených ľudských zdrojov a uchovávanie výsledkov posúdení vplyvu AI systémov na účely ďalšieho zlepšovania. Súčasťou musí byť aj neustále zdokonaľovanie prevádzky a definovanie procesov pre zodpovedné používanie AI systémov.

V nasledujúcej kapitole uvádzame zoznam (checklist) jednotlivých bezpečnostných opatrení pre systémy AI vo fáze zlepšovania systémov AI a reakcie na incidenty s odkazom na prislúchajúcu časť normy ISO/EIC 42001:2023). **V prílohe D** je uvedené úplné mapovanie jednotlivých ustanovení ZoITVS k norme ISO/EIC 42001:2023.

4.8.1 BEZPEČNOSTNÉ OPATRENIA

Správca informačných technológií verejnej správy by mal vykonať nasledujúce bezpečnostné opatrenia:

- určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI (ISO/IEC 42001:2023 – A.8.4 Communication of incidents),
- politika AI by sa mala preskúmavať v plánovaných intervaloch alebo dodatočne podľa potreby, aby sa zabezpečila jej trvalá vhodnosť, primeranosť a účinnosť (ISO/IEC 42001:2023 – A.2.4 Review of the AI policy),
- ako súčasť identifikácie zdrojov dokumentovať informácie o ľudských zdrojoch a ich kompetenciách využívaných na vývoj, nasadenie, prevádzku, riadenie zmien, údržbu, prenos a vyraďovanie systému AI, ako aj na overovanie a integráciu systému AI (ISO/IEC 42001:2023 – A.4.6),
- definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI (ISO/IEC 42001 – A.6.2.6),
- zdokumentovať výsledky posúdení vplyvu systému AI a uchovávať výsledky počas vymedzeného obdobia (ISO/IEC 42001:2023 – A.5.3 Documentation of AI system impact assessments),
- definovať a dokumentovať procesy pre zodpovedné používanie systémov AI (ISO/IEC 42001:2023 – A.9.2 Processes for responsible use of AI systems),
- definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu (ISO/IEC 42001:2023 – A.6.2.6 AI system operation and monitoring).

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

4.8.2 PRÍPADOVÉ ŠTÚDIE

AI nástroj na úpravu fotografií

Správca ITVS musí pravidelne aktualizovať AI politiku na základe skúseností z prevádzky, napr. identifikovaných problémov s kvalitou obrazu (A.2.4). Musí zabezpečiť, že používatelia majú potrebné kompetencie na správne používanie nástroja (A.4.6). Výsledky impact assessment musia byť dokumentované, napr. prípady, kde došlo k zmene významu obrázka (A.5.3). Na základe monitorovania musí optimalizovať model alebo parametre spracovania (A.6.2.6).

AI chatbot pre komunikáciu s občanmi

Organizácia musí pravidelne aktualizovať AI politiku chatbotu na základe nových hrozieb, napr. nových typov prompt injection útokov (A.2.4). Musí evidovať kompetencie zamestnancov zodpovedných za správu a bezpečnosť AI systému (A.4.6). Výsledky impact assessment (napr. dopad nesprávnych odpovedí na občanov) musia byť dokumentované a archivované (A.5.3). Na základe incidentov a monitoringu musí organizácia zlepšovať model, filtre a bezpečnostné opatrenia (A.6.2.6). Súčasne musí aktualizovať pravidlá používania systému (A.9.2).

Systém AI pre triedenie uchádzačov o zamestnanie

Musí pravidelne aktualizovať AI politiku na základe nových legislatívnych požiadaviek alebo identifikovaných rizík diskriminácie (A.2.4). Musí zabezpečiť, že pracovníci HR a IT majú potrebné kompetencie na interpretáciu výstupov AI systému (A.4.6). Výsledky AI impact assessment musia byť dokumentované a použité na úpravu modelu alebo procesov (A.5.3). Na základe monitorovania musí optimalizovať model, napr. re-trénovaním na vyvážených datasetoch (A.6.2.6).

4.8.3 PRÍKLAD DOKUMENTÁCIE

Pre zlepšovanie bezpečnosti AI systémov a reakciu na incidenty (fáza ACT) môže správca informačných technológií verejnej správy prijať nasledujúce riadiace dokumenty:

- **Post-incident report** – analyzuje príčiny incidentov a identifikuje opatrenia na ich prevenciu. Slúži ako vstup pre zlepšovanie AIMS. Väzba na ISO/IEC 42001:2023 - A.8.4.
- **Plán nápravných a preventívnych opatrení** – definuje opatrenia na odstránenie príčin nesúladu a prevenciu opakovania. Podporuje systematické zlepšovanie. Väzba na ISO/IEC 42001:2023 - kap. 10.2.
- **Management review AIMS** – pravidelné hodnotenie systému riadenia AI vrcholovým manažmentom. Posudzuje efektívnosť, riziká a príležitosti na zlepšenie. Väzba na ISO/IEC 42001:2023 - kap. 9.3.
- **Revízia AI politiky** – aktualizácia politiky na základe zmien v prostredí, legislatíve alebo výsledkov auditov. Zabezpečuje jej aktuálnosť a účinnosť. Väzba na ISO/IEC 42001:2023 - A.2.4.
- **Plán vyradenia systému AI** – definuje postupy bezpečného ukončenia prevádzky systému AI vrátane správy dát a zdrojov. Minimalizuje riziká pri ukončení životného cyklu. Väzba na ISO/IEC 42001:2023 - A.6.2.6, A.4.6.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

- **Program neustáleho zlepšovania AIMS** – systematizuje aktivity na zvyšovanie efektívnosti a bezpečnosti AI. Vychádza z auditov, incidentov a metrík. Väzba na ISO/IEC 42001:2023 - kap. 10.1.
- **Školenia a povedomie o AI bezpečnosti** – zabezpečuje vzdelávanie zamestnancov o bezpečnom a etickom používaní AI. Podporuje kultúru zodpovedného využívania AI. Väzba na ISO/IEC 42001:2023 - A.9.2.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

POUŽITÉ ZDROJE

[1] GDPRLocal. (2025, 3. november). *AI risk classification: Guide to EU AI Act risk categories*. https://gdprlocal.com/ai-risk-classification/

[2] Google. (n.d.). *Components of generative AI systems*. Secure AI Framework (SAIF). https://saif.google/secure-ai-framework/components

[3] International Organization for Standardization, & International Electrotechnical Commission. (2022). *ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*. ISO.

[4] International Organization for Standardization & International Electrotechnical Commission. (2023). *ISO/IEC 42001:2023 Informačné technológie — Umelá inteligencia — Systém manažérstva*. ISO.

[5] MITRE. (n.d.). *MITRE ATLAS: Adversarial Threat Landscape for Artificial-Intelligence Systems*. Retrieved from https://atlas.mitre.org/

[6] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej aj „GDPR“).

[7] Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (ďalej aj „AI akt“ alebo „AIA“),

[8] National Institute of Standards and Technology. (2023). *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations* (NIST AI 100-2e2023). https://doi.org/10.6028/NIST.AI.100-2e2023

[9] OWASP Foundation. (2023). *OWASP Top 10 for Large Language Model Applications*. Retrieved from https://owasp.org/www-project-top-10-for-large-language-model-applications/

[10] Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,

[11] Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.

PRÍLOHA A

PDCA fáza	Ustanovenie ZoITVS	Znenie ZoITVS	Norma ISO/IEC 42001:2023	Norma ISO/IEC 42001:2023 – bezpečnostné opatrenie
PLAN	§18 ods.1	Povinnosť správcu, ktorý je prevádzkovateľom základnej služby, prijať a realizovať bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe v závislosti od klasifikácie informácií a kategorizácie sietí a informačných systémov ustanovuje osobitný predpis.	N/A	N/A
PLAN	§18 ods.2	Správca, ktorý je prevádzkovateľom základnej služby, prijíma a realizuje bezpečnostné opatrenia vo vzťahu k informačným systémom verejnej správy v jeho správe podľa tohto zákona a osobitného predpisu, ak ich cieľom je dosiahnuť vyššiu úroveň bezpečnosti ako ustanovuje osobitný predpis.	N/A	N/A
PLAN	§19 ods.1 písm. a)	Určiť ciele, rozsah, podmienky, povinnosti osôb, ktoré vykonávajú činnosť pre správcu a organizačných zložiek správcu a prostriedky riadenia bezpečnosti vo forme bezpečnostnej dokumentácie schválených procesov riadenia bezpečnosti informačných technológií verejnej správy.	A.2.2 AI policy	Organizácia musí zdokumentovať politiku pre vývoj alebo používanie systémov AI.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PLAN	§19 ods.1 písm. b)	Zriadiť riadiacu, výkonnú a kontrolnú zložku systému riadenia bezpečnosti, ktoré sú navzájom personálne a kompetenčne oddelené.	A.3.2 AI roles and responsibilities	Roly a zodpovednosti pre AI musia byť definované a pridelené podľa potrieb organizácie.
PLAN	§19 ods.1 písm. c)	Zabezpečiť a zdokumentovať identifikáciu aktív v ITVS a riadenie rizík, najmä vo forme bezpečnostnej dokumentácie vrátane bezpečnostného projektu.	A.4.2 Resource documentation	Organizácia musí identifikovať a dokumentovať relevantné zdroje potrebné pre činnosti v daných fázach životného cyklu systému AI a ďalšie činnosti súvisiace s AI, ktoré sú pre organizáciu relevantné.
PLAN	§19 ods.1 písm. d)	Určiť a zaviesť bezpečnostné opatrenia na procesnej, organizačnej a technickej úrovni.	A.6.1.3 Processes for responsible AI system design and development	Organizácia musí definovať a dokumentovať konkrétne procesy pre zodpovedný návrh a vývoj systému AI.
PLAN	§19 ods.1 písm. e)	Určiť prostriedky a zdroje na zabezpečenie implementácie a riadneho fungovania bezpečnostných opatrení.	A.4.2 Resource documentation	Organizácia musí identifikovať a dokumentovať relevantné zdroje potrebné pre činnosti v daných fázach životného cyklu systému AI a ďalšie činnosti súvisiace s AI, ktoré sú pre organizáciu relevantné.
PLAN	§19 ods.1 písm. f)	Určiť prostriedky kontroly uplatňovania bezpečnostných opatrení.	A.6.2.4 AI system verification and validation	Organizácia musí definovať a dokumentovať opatrenia overovania a validácie pre systém AI a špecifikovať kritériá ich použitia.
PLAN	§19 ods.1 písm. g)	Určiť postupy riešenia bezpečnostných incidentov.	A.8.4 Communication of incidents	Organizácia musí určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI.
PLAN	§19 ods.5 písm. a)	Dodržiavať bezpečnostnú stratégiu kybernetickej bezpečnosti.	A.2.3 Alignment with other organizational policies	Organizácia musí určiť, kde môžu byť iné organizačné politiky ovplyvnené cieľmi organizácie vo vzťahu k systémom AI alebo kde sa na ne tieto ciele uplatňujú.
PLAN	§19 ods.5 písm. b)	Určiť osobu zodpovednú za bezpečnosť ISVS.	A.3.2 AI roles and responsibilities	Roly a zodpovednosti pre AI musia byť definované a pridelené podľa potrieb organizácie.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PLAN	§19 ods.5 písm. c)	Identifikovať riziká prostredia, v ktorom bude ISVS prevádzkovaný.	A.5.2 AI system impact assessment process	Organizácia musí zaviesť proces na posudzovanie možných dôsledkov pre jednotlivcov alebo skupiny jednotlivcov, alebo pre oboje, a spoločnosti, ktoré môžu vyplynúť zo systému AI počas celého jeho životného cyklu.
PLAN	§23 ods.2	Identifikácia kritických ISVS pri vypracovaní bezpečnostného projektu pre ISVS (pri narušení bezpečnosti môže spôsoboiť závažný KBI, tvorí základné alebo referenčné registre, je agendový systém, je nevyhnutný na rozhodovanie orgánu verejnej moci, je špecializovaný portál, spracúva osobitné kategórie osobných údajov, je zaradený do kategórie III.)	A.5.2 AI system impact assessment process	Organizácia musí zaviesť proces na posudzovanie možných dôsledkov pre jednotlivcov alebo skupiny jednotlivcov, alebo pre oboje, a spoločnosti, ktoré môžu vyplynúť zo systému AI počas celého jeho životného cyklu.
PLAN	§23 ods.3 písm. c)	Zasielať orgánu vedenia najmenej jedenkrát do roka zoznam aktív.	A.4.2 Resource documentation	Organizácia musí identifikovať a dokumentovať relevantné zdroje potrebné pre činnosti v daných fázach životného cyklu systému AI a ďalšie činnosti súvisiace s AI, ktoré sú pre organizáciu relevantné.
PLAN	§23 ods.3 písm. d)	Zasielanie informácií o aktívach, rizikách, kontaktných bodoch a evidencii KBI ITVS vládnej jednotke CSIRT v stanovenom rozsahu.	A.3.3 Reporting of concerns	Organizácia musí definovať a zaviesť proces na oznamovanie obáv týkajúcich sa úlohy organizácie vo vzťahu k systému AI počas celého jeho životného cyklu.
PLAN	§23 ods.3 písm. e)	Zverejňovanie na svojom webovom sídle pravidlá na oznamovanie zraniteľností.	A.10.2 Allocating responsibilities	Organizácia musí zabezpečiť, aby boli zodpovednosti v rámci životného cyklu systému AI rozdelené medzi organizáciu, jej partnerov, dodávateľov, zákazníkov a tretie strany.

PLAN	§23 ods.5 písm. b)	Bezodkladné riešenie KBI a prijať opatrenia na zníšenie rizika vyplývajúceho zo zraniteľnosti.	A.8.5 Information for interested parties	Organizácia musí určiť a zdokumentovať svoje povinnosti týkajúce sa oznamovania informácií o systéme AI zainteresovaným stranám.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍLOHA B

PDCA fáza	Ustanovenie ZoITVS	Znenie ZoITVS	Norma ISO/IEC 42001:2023	Norma ISO/IEC 42001:2023 – bezpečnostné opatrenie
DO	§20 ods.1 písm. a)	Určiť bezpečnostné požiadavky na ISVS vrátane podmienok jeho vývoja, testovania a dodania v podmienkach vytvorenia alebo dodania ISVS.	A.6.2.2 AI system requirements and specification	Organizácia musí špecifikovať a dokumentovať požiadavky na nové systémy AI alebo podstatné vylepšenia existujúcich systémov.
DO	§20 ods.1 písm. b)	Zabezpečiť pre tento systém vypracovanie bezpečnostnej dokumentácie vrátane bezpečnostného projektu.	A.6.2.3 Documentation of AI system design and development	Organizácia musí dokumentovať návrh a vývoj systému AI na základe organizačných cieľov, zdokumentovaných požiadaviek a kritérií špecifikácie.
DO	§20 ods.2 písm. a)	Zabezpečiť bezpečné vývojové prostredie a dokumentáciu vývoja a testovania vrátane používateľskej a administrátorskej dokumentácie.	A.6.1.3 Processes for responsible AI system design and development	Organizácia musí definovať a dokumentovať konkrétne procesy pre zodpovedný návrh a vývoj systému AI.
DO	§20 ods.2 písm. b) bod 1	Dodávateľ je povinný dodržiavať mlčanlivosť o informačnom systéme aj po ukončení dodania a zaviazať tým všetky zúčastnené osoby.	N/A	N/A
DO	§20 ods.2 písm. b) bod 2	Doplniť bezpečnostné požiadavky na ISVS a predložiť správcovi návrh bezpečnostných opatrení na naplnenie týchto bezpečnostných požiadaviek pre prostredie, v ktorom bude ISVS prevádzkovaný.	A.6.2.5 AI system deployment	Organizácia musí zdokumentovať plán nasadenia a zabezpečiť, aby boli pred nasadením splnené príslušné požiadavky.
DO	§20 ods.2 písm. b) bod 3	Preukázateľne odstrániť alebo znemožniť používanie funkcie ISVS umožňujúce neoprávnený prístup do systému alebo jeho údajom.	N/A	N/A

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DO	§21 ods.1	Zavedenie, prevádzka a vyradenie ISVS.	A.6.2.5 / A.6.2.6	Organizácia musí zdokumentovať plán nasadenia a zabezpečiť, aby boli pred nasadením splnené príslušné požiadavky. / Organizácia musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu.
DO	§21 ods.2 písm. a)	Overiť splnenie funkčných, výkonnostných a bezpečnostných požiadaviek pred zavedením do prevádzky a nezavedenie ISVS, ktorý požiadavky nespĺňa.	A.6.2.4 AI system verification and validation	Organizácia musí definovať a dokumentovať opatrenia overovania a validácie pre systém AI a špecifikovať kritériá ich použitia.
DO	§21 ods.2 písm. b)	Vykonať bezpečnostné testovanie ISVS, ktorý má rozhranie s verejnou sieťou Internet a ktorý spracúva osobné údaje alebo chránené či prísne chránené informácie	A.6.2.4 AI system verification and validation	Organizácia musí definovať a dokumentovať opatrenia overovania a validácie pre systém AI a špecifikovať kritériá ich použitia.
DO	§23 ods.5 písm. e)	Prijatie alebo úprava bezpečnostných opatrení po riešení bezpečnostného incidentu, penetračnom testovaní, hodnotení zraniteľností alebo posúdení bezpečnosti IT alebo IS orgánu riadenia.	N/A	N/A
DO	§23 ods.5 písm. g)	Určenie a zverejnenie na svojom hlavnom webovom sídle kontaktné údaje na kontaktný bod na nahlasovanie kybernetického bezpečnostného incidentu.	N/A	N/A
DO	§23 ods.3 písm. a)	Nahlasovať kybernetické bezpečnostné incidenty ak je orgán riadenia zaradený do registra PZS alebo PDS príslušným spôsobom.	A.8.4 Communication of incidents	Organizácia musí určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍLOHA C

PDCA fáza	Ustanovenie ZoITVS	Znenie ZoITVS	Norma ISO/IEC 42001:2023	Norma ISO/IEC 42001:2023 – bezpečnostné opatrenie
CHECK	§21 ods.3 písm. a)	Zabezpečiť určenie, pravidelnú aktualizáciu bezpečnostnej dokumentácie a dodržiavanie bezpečnostných opatrení.	A.6.2.7 AI system technical documentation	Organizácia musí určiť, aká technická dokumentácia systému AI je potrebná pre každú relevantnú kategóriu zainteresovaných strán, ako sú používatelia, partneri, dozorné orgány, a poskytnúť im technickú dokumentáciu vo vhodnej forme.
CHECK	§21 ods.3 písm. b) bod 5	Zabezpečiť nepretržitý monitoring ISVS.	A.6.2.6 AI system operation and monitoring	Organizácia musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu.
CHECK	§21 ods.3 písm. b) bod 6	Zabezpečiť pravidelný bezpečnostný audit v pravidelných intervaloch a aktualizáciu bezpečnostného projektu pri zistení závažných nedostatkov.	N/A	N/A
CHECK	§22	Prijímať a vykonávať bezpečnostné opatrenia v oblasti monitorovania, testovania bezpečnosti a bezpečnostných auditov.	A.6.2.6 AI system operation and monitoring	Organizácia musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu.
CHECK	§23 ods.5 písm. f)	Viesť evidenciu KBI, postupov na riešenie KBI	A.8.4 Communication of incidents	Organizácia musí určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CHECK	§23a ods.2 písm. a)	Vykonávať činnosti nepretržitého monitorovania ITVS na žiadosť správcu.	A.9.2 Processes for responsible use of AI systems	Organizácia musí definovať a dokumentovať procesy pre zodpovedné používanie systémov AI.
CHECK	§23a ods.2 písm. b)	Vykonávať pravidelné neinvazívne hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb	A.6.2.6 AI system operation and monitoring	Organizácia musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu.
CHECK	§23a ods.2 písm. c)	Hodnotenie zraniteľnosti služby verejnej správy, služby vo verejnom záujme, verejnej služby a ďalších služieb so súhlasom správcu.	A.8.4 Communication of incidents	Organizácia musí určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI.
CHECK	§23 ods.5 písm. a)	Nahlasovanie KBI vládnej jednotke CSIRT.	A.3.3 Reporting of concerns	Organizácia musí definovať a zaviesť proces na oznamovanie obáv týkajúcich sa úlohy organizácie vo vzťahu k systému AI počas celého jeho životného cyklu.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÍLOHA D

PDCA fáza	Ustanovenie ZoITVS	Znenie ZoITVS	Norma ISO/IEC 42001:2023	Norma ISO/IEC 42001:2023 – bezpečnostné opatrenie
ACT	§19 ods.2 písm. b)	Zabezpečiť prerokovanie a schválenie informácií o závažných bezpečnostných incidentoch spolu s návrhom opatrení na minimalizáciu och opätovného výskytu.	A.8.4 Communication of incidents	Organizácia musí určiť a zdokumentovať plán komunikovania incidentov používateľom systému AI.
ACT	§19 ods.2 písm. c)	Zabezpečiť prerokovanie a schválenie návrhu opatrení vyplývajúcich z analýz, riešených bezpečnostných incidentov, havarijných stavov, kontrol a auditov.	A.2.4 Review of the AI policy	Politika AI sa musí preskúmavať v plánovaných intervaloch alebo dodatočne podľa potreby, aby sa zabezpečila jej trvalá vhodnosť, primeranosť a účinnosť.
ACT	§21 ods.4	Vypracovať plán vyradenia ISVS z prevádzky vrátane uchovania informácií, ich spoľahlivého odstránenia a postupu vyraďovania programových a technických prostriedkov ISVS.	A.4.6 / A.6.2.6	Organizácia musí ako súčasť identifikácie zdrojov dokumentovať informácie o ľudských zdrojoch a ich kompetenciách využívaných na vývoj, nasadenie, prevádzku, riadenie zmien, údržbu, prenos a vyraďovanie systému AI, ako aj na overovanie a integráciu systému AI. / Organizácia musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu.
ACT	§23 ods.1	Vypracovanie bezpečnostného projektu ISVS vychádzajúc z bezpečnostnej stratégie, bezpečnostných politík, všeobecne akceptovaných štandardov a metodických usmernení orgánu vedenia.	A.5.3 Documentation of AI system impact assessments	Organizácia musí zdokumentovať výsledky posúdení vplyvu systému AI a uchovávať výsledky počas vymedzeného obdobia.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ACT	§23a ods.1 písm. a)	Metodické usmerňovanie správcov na účely dosiahnutia a udržania bezpečnosti ITVS a zvyšovanie povedomia správcov a verejnosti.	A.9.2 Processes for responsible use of AI systems	Organizácia musí definovať a dokumentovať procesy pre zodpovedné používanie systémov AI.
ACT	§23a ods.2 písm. e)	Vykonávanie činností na účely riešenia KBI, jeho predchádzania alebo odstraňovania a hodnotenia zraniteľnosti na žiadosť orgánu riadenia.	A.6.2.6 AI system operation and monitoring	Organizácia musí definovať a dokumentovať potrebné prvky pre priebežnú prevádzku systému AI. Minimálne to má zahŕňať monitorovanie systému a výkonnosti, opravy, aktualizácie a podporu.