

„Štúdia uskutočniteľnosti implementácie experimentálneho regulačného rámca v oblasti AI“

OBSAH

Úvod	2
Manažérske zhrnutie	2
1. Komplexná štúdia pripravovaných európskych predpisov a ich dopad na SR	5
1.1. Analýza právneho rámca EÚ vo vzťahu k základnými právam a bezpečnostným rizikám špecifickým pre systémy umelej inteligencie	5
1.2. Pravidlá EÚ na riešenie otázok zodpovednosti v súvislosti s novými technológiami vrátane systémov umelej inteligencie	13
1.3. Prehľad základných sektorových bezpečnostných právnych predpisov relevantných v kontexte Nariadenia a zriaďovania sandboxov - môže podliehať ďalšej úprave	14
2 Analýza dotknutých subjektov na strane orgánov verejnej moci, regulovaných subjektov a ostatných zainteresovaných osôb vo vzťahu k implementácii sandboxu (experimentálneho regulačného prostredia) v prostredí Slovenskej republiky	17
2.1 Analýza orgánov verejnej moci v rámci SR, ktoré sú príslušné na implementovanie Nariadenia alebo ich spolupráca bude potrebná na zabezpečenie fungovania sandboxu	17
2.2 Zodpovednosti aktérov realizácie sandboxu pre umelú inteligenciu predpokladaného Nariadením	28
2.3 Analýza dopadov zavedenia experimentálneho regulačného prostredia (sandboxu) na dotknuté zainteresované osoby	30
3 Analýza súčasného stavu implementácie riešení umelej inteligencie (AI) a právneho rámca pre zriadenie sandboxov v zmysle Nariadenia a slovenskej legislatívy	34
3.1 Analýza súčasného stavu právneho rámca implementácie AI riešení na Slovensku	34
3.2 Analýza existujúcich experimentálnych regulačných prostredí (sandboxov) z 2 iných jurisdikcií, ktoré zaviedli regulačné opatrenia v oblasti AI	50
3.3 Odporúčania pre zriadenie sandboxu pre umelú inteligenciu v prostredí Slovenskej republiky	56
4 Analýza náročnosti implementácie experimentálneho regulačného prostredia (sandboxu) v prostredí SR	66
4.1 Vyhodnotenie náročnosti vytvorenia a prevádzky experimentálneho regulačného prostredia podľa požiadaviek pripravovanej európskej legislatívy a relevantných osvedčených postupov.	66
4.2 Zhodnotenie aktuálneho regulačného prostredia vo vzťahu k zriadeniu sandboxu pre umelú inteligenciu v prostredí SR a identifikácia materiálnych právno-legislatívnych rizík na zohľadnenie vo vzťahu k zriaďovaniu sandboxu pre umelú inteligenciu	66

4.3	Analýza požadovaného organizačného zabezpečenia potrebného pre fungovanie experimentálneho regulačného prostredia.	68
4.4	Stanovenie alternatív podoby implementácie sandboxu pre umelú inteligenciu v zmysle Nariadenia a výber odporúčaného budúceho riešenia.	70
4.5	Identifikácia technického riešenia na základe analýzy požiadaviek.	70
4.6	Detekcia základných rizík a prekážok, ktoré môžu zabrániť alebo skomplikovať implementáciu sandboxu pre umelú inteligenciu v zmysle Nariadenia v prostredí SR	71
5	Analýza identifikovaného technického riešenia	74
5.1	Návrh technického riešenia z pohľadu dizajnu, infraštruktúry a funkčných požiadaviek na sandbox pre umelú inteligenciu v zmysle Nariadenia	74
5.2	Stanovenie variantov technologického riešenia sandboxu pre umelú inteligenciu v zmysle Nariadenia	87
5.3	Stanovenie kritérií pre výber variantu technologického riešenia podpory AI sandboxu	88
5.4	Základné používateľské prípady	90
5.5	Návrh technického riešenia podpory sandboxu pre umelú inteligenciu v zmysle Nariadenia z pohľadu požiadaviek	94
5.6	Prehľad nákladovej štruktúry pre zvolenú alternatívu a analýza nákladov na implementáciu a prevádzku sandboxu pre umelú inteligenciu (v zmysle Nariadenia)	99
5.7	Časový rámec	103
5.8	Cestovná mapa implementácie a Návrh postupu implementácie regulačného experimentálneho prostredia	107
6	Limitácie	108

Úvod

Táto štúdia je vyhotovená na základe objednávky č.1000028737 zo dňa 9.11.2023 medzi Ministerstvom investícií, regionálneho rozvoja a informatizácie SR (ďalej len „**MIRRI**“) a PricewaterhouseCoopers Slovensko, s.r.o (ďalej len „**PwC**“), pričom jej obsahom je štúdia uskutočniteľnosti implementácie experimentálneho regulačného rámca pre umelú inteligenciu v prostredí SR (ďalej len „**Štúdia**“). Štruktúra Štúdie a jej časti (s výnimkou Manažérskeho zhrnutia) z obsahového hľadiska zodpovedá štruktúre „Oblasti poradenských služieb“ uvedených vo Výzve na predkladanie ponúk MIRRI zo dňa 19.10.2023, pričom rozsah a definícia obsahu zadania je zodpovednosťou MIRRI.

Postupy týkajúce sa prípravy Štúdie sme vykonali v období od 9.11.2023 do 14.12.2023. Rozsah nami vykonaných prác pozostával z analýzy verejne dostupných informácií a dostupných návrhov legislatívnych aktov v čase prípravy tejto Štúdie. Podrobné obmedzenia sú uvedené podrobne v časti „Limitácie“ Štúdie. Podrobnosti o použitých postupoch, zdrojoch informácií, z ktorých sme čerpali, a zisteniach sú opísané v ďalších častiach tohto dokumentu.

Manažérske zhrnutie

Hlavným právnym predpisom upravujúcim reguláciu systémov umelej inteligencie v rámci Európskej únie (ďalej len „**EÚ**“), bude po jeho prijatí Nariadenie Európskeho parlamentu a Rady, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie (ďalej len „**Nariadenie**“)¹, ktoré je aktuálne v legislatívnom procese s očakávanou účinnosťou začiatkom roka 2024. Jedným z regulačných nástrojov, ktoré Nariadenie zavádza sú tzv. „experimentálne regulačné prostredia“ (sandboxy)², ktoré predstavujú kontrolované prostredia vytvorené verejným orgánom, ktoré uľahčujú bezpečný vývoj, testovanie a validáciu inovatívnych systémov umelej inteligencie na obmedzený čas pred ich uvedením na trh alebo do prevádzky podľa konkrétneho plánu pod regulačným dohľadom.

Táto Štúdia hodnotí uskutočniteľnosť zriadenia sandboxu pre umelú inteligenciu (v zmysle Nariadenia) v prostredí Slovenskej republiky (ďalej aj ako „**SR**“) vo všeobecnosti bez ohľadu na to, či zriadenie sandboxu pre umelú inteligenciu členskými štátmi EÚ bude na základe finálneho textu Nariadenia povinné alebo dobrovoľné.

Čo sa týka legislatívno-technických aspektov zriaďovania AI sandboxov, Nariadenie aktuálne neupravuje konkrétny postup ani formu, ktorou má byť sandbox (resp. sandboxy) pre umelú inteligenciu v prostredí konkrétneho členského štátu EÚ zriadený. S prihliadnutím na uvedené teda Slovenská republika (i) má značnú voľnosť akým spôsobom ciele a požiadavky Nariadenia vo vzťahu k zriadeniu a fungovaniu AI sandboxu naplní (pri rešpektovaní požiadaviek na fungovanie AI sandboxu stanovených Nariadením) a (ii) môže si vybrať najvhodnejší spôsob zohľadňujúci okrem iného preferovanú štruktúru inštitucionálneho rámca pre aplikáciu Nariadenia (viď aj časť 2.1 Štúdie nižšie). Keďže však legislatívny proces vo vzťahu k Nariadeniu v čase prípravy Štúdie nebol ukončený a Nariadenie predpokladá aj následné vydanie delegovaného aktu zo strany Európskej komisie (ďalej

¹ Ako bude bližšie vysvetlené v časti 1.1 s prihliadnutím na praktické a časové implikácie prípravy Štúdie, Štúdia vychádza z návrhu Nariadenia v znení pozmeňujúcich návrhov prijatých Európskym parlamentom 14. júna 2023.

² V rámci Štúdie používame pre označenie experimentálnych regulačných prostredí primárne pojem „sandbox“ a pre sandboxy pre oblasť umelej inteligencie pojem „sandbox pre umelú inteligenciu“ alebo „AI sandbox“.

len „Komisia“) bližšie upravujúceho otázky zriaďovania AI sandboxov, bude potrebné ďalej sledovať legislatívne procesy a flexibilne reagovať na prípadné zmeny a/alebo dodatočné špecifikácie z nich vyplývajúce.

Z analýzy existujúceho právneho rámca máme za to, že v súčasnosti neexistujú materiálne legislatívne prekážky pre zriadenie a fungovanie AI sandboxu predpokladaného Nariadením. To potvrdzuje aj aktuálne pôsobenie regulačných sandboxov Národnej banky Slovenska (ďalej len „NBS“) a Úradu pre reguláciu sieťových odvetví (ďalej len „ÚRSO“) v právnom prostredí Slovenskej republiky. Na druhej strane konkrétne špecifiká pre zriadenie a fungovanie AI sandboxu a výber najvhodnejšieho riešenia budú závisieť aj od toho akým spôsobom budú implementované požiadavky Nariadenia najmä vo vzťahu k inštitucionálnemu rámcu predpokladanému Nariadením do existujúceho legislatívneho a inštitucionálneho rámca Slovenskej republiky (najmä čo sa týka určenia príslušného vnútroštátneho dozorného orgánu a/alebo orgánu zriaďujúceho AI sandbox a nastavenia spolupráce s ostatnými orgánmi verejnej moci (ďalej aj ako „OVM“), a to okrem iného po zohľadnení záverov a odporúčaní TSI Analýzy (ako je definovaná nižšie).

S prihliadnutím na praktické a systematické aspekty (najmä pôsobnosť v oblasti vydávania usmernení a poradenstva týkajúceho sa vykonávania Nariadenia a dohľadu a kontroly v oblasti pôsobnosti Nariadenia) odporúčame zväziť zriadenie AI sandboxu v rámci pôsobnosti už existujúceho OVM, ktorý bude určený Slovenskou republikou ako vnútroštátny dozorný orgán v zmysle Nariadenia, a ktorý pre tieto účely bude môcť (okrem iného) využiť aj svoje existujúce kapacity, ak nebudú identifikované dôvody, pre ktoré by mal byť zriaďujúcim orgánom AI sandboxu iný OVM SR.

Pre zriadenie AI sandboxu v prostredí SR navrhujeme zväziť kombináciu legislatívno-technických nástrojov uvedených v časti 3.1.3 Štúdie, vrátane rámcovej zákonnej úpravy AI sandboxu formou tzv. experimentálnej doložky³ a s konkrétnejšou reguláciou praktických aspektov fungovania AI sandboxu (najmä pravidiel prihlasovania, hodnotenia kritérií a pod.) formou iných vykonávacích regulačných aktov príslušného orgánu (resp. orgánov) umožňujúcich vyššiu flexibilitu reagovania na prípadné zmeny alebo požiadavky súvisiace s fungovaním sandboxu.

V Štúdii popisujeme príklady sandbox riešení zo sveta, získané z verejne dostupných zdrojov, pričom primárne sa venuje existujúcim riešeniam v Španielsku a Spojenom kráľovstve. Následne v Štúdii uvádzame odporúčania, ktoré vyplývajú z aktuálneho legislatívneho nastavenia, ale najmä posudzovaných existujúcich riešení. Odporúčania predpokladajú tri fázy projektu v AI sandboxe: 1. Príprava, 2. Realizácia a 3. Vyhodnotenie, ako aj periodické vyhodnocovanie samotného existujúceho AI sandboxu. K návrhu organizačného zabezpečenia pristupujeme prostredníctvom návrhu potrebných personálnych kapacít, a technických požiadaviek.

Pre zabezpečenie technickej podpory AI sandboxu je v rámci tejto Štúdie navrhnutý informačný systém, ktorý vytvorí prostredie pre podporu validácie a testovania AI riešení na báze riadenej kolaborácie zainteresovaných účastníkov. Systém umožní konfiguráciu postupov, pracovných tokov

³ T.j. základná rámcová úprava kompetencií súvisiacich s AI sandboxom napr. formou vloženia príslušných zákonných ustanovení upravujúcich základný rámec fungovania AI sandboxu do zákona zavádzajúceho právomoci vnútroštátneho dozorného orgánu v zmysle Nariadenia.

(workflow), správy dát a bezpečnosti. Návrh požiadaviek na informačný systém vychádza predovšetkým z funkcií a kompetencií AI sandboxu podľa Nariadenia.

Vyššie uvedené návrhy a odporúčania budú vyžadovať investičné a prevádzkové náklady, ktoré sú odhadnuté v časti Štúdie 5.6. Odhad predpokladaných nákladov pozostáva zo zriadenia organizácie a realizácie súvisiaceho informačného systému, čiže projektovej časti, ako aj z odhadov nákladov pre následnú prevádzku.

1. Komplexná štúdia pripravovaných európskych predpisov a ich dopad na SR

1.1. Analýza právneho rámca EÚ vo vzťahu k základnými právam a bezpečnostným rizikám špecifickým pre systémy umelej inteligencie⁴

V rámci tejto časti Štúdie v prvom rade (i) sumarizujeme aktuálny stav legislatívy na úrovni EÚ v oblasti regulácie systémov umelej inteligencie vo všeobecnosti (časť 1.1.1 nižšie), (ii) uvádzame zhrnutie základných aspektov Nariadenia, ktoré po jeho prijatí bude hlavným právnym predpisom upravujúcim reguláciu systémov umelej inteligencie v rámci EÚ, vrátane povinností členských štátov v oblasti zriaďovania „experimentálnych regulačných prostredí“ (sandboxov) pre umelú inteligenciu⁵ relevantných pre implementáciu sandboxov (časť 1.1.2 nižšie), a (iii) následne analyzujeme základné povinnosti pre SR ako členský štát EÚ v kontexte Nariadenia (časť 1.1.3 nižšie), ktoré sú ďalej rozvinuté v ďalších častiach Štúdie (najmä časť 2 nižšie).

V čase prípravy tejto Štúdie bol text Nariadenia stále v legislatívnom procese. Napriek tomu, že k politickej dohode Európskeho parlamentu a Rady na finálnom znení Nariadenia došlo dňa 8. decembra 2023, k dátumu vyhotovenia tejto Štúdie, nebolo k dispozícii finálne konsolidované znenie Nariadenia, pričom podľa verejne dostupných informácií bol odhadovaný časový rámec na prípravu finálneho znenia Nariadenia minimálne v trvaní niekoľkých týždňov (s predpokladanou dostupnosťou konsolidovaného znenia v priebehu januára 2024).⁶ S prihliadnutím na uvedené ako aj praktické a časové implikácie prípravy Štúdie a predpoklad, že základné východiská relevantné pre posúdenie uskutočniteľnosti sandboxu pre umelú inteligenciu v prostredí Slovenskej republiky by nemali byť zásadne dotknuté, bolo dohodnuté, že Štúdia bude vychádzať zo znenia návrhu Nariadenia v znení pozmeňujúcich návrhov prijatých Európskym parlamentom 14. júna 2023⁷, pričom tento postup bol potvrdený zo strany MIRRI.⁸

V súvislosti s vyššie uvedeným upozorňujeme, že je možné, že v rámci finalizácie textu Nariadenia môže dôjsť k určitým úpravám textu s vplyvom na niektoré aspekty Štúdie, vrátane zmeny rozsahu povinností a kompetencií vnútroštátnych orgánov, a to vo všeobecnosti ako aj vo vzťahu k určitým aspektom zriaďovania a fungovania AI sandboxov. V tomto ohľade bude potrebné naďalej sledovať legislatívny proces súvisiaci s Nariadením a akékoľvek dodatočne špecifikované a/alebo zmenené požiadavky z neho vyplývajúce zohľadniť v rámci procesu hodnotenia a rozhodovania o preferovanej forme zriadenia sandboxu pre umelú inteligenciu v prostredí SR.

⁴ V angličtine „artificial intelligence“ (ďalej aj len „AI“).

⁵ V rámci Štúdie používame pre označenie experimentálnych regulačných prostredí primárne pojem sandbox a pre sandboxy pre oblasť umelej inteligencie pojem „sandbox pre umelú inteligenciu“ alebo „AI sandbox“.

⁶ Viď napr. https://www.linkedin.com/posts/walter-m-pasquarelli_aiact-eu-aipolicy-activity-7139916987060641792-giHP/?utm_source=share&utm_medium=member_desktop

⁷ Viď dokument so zn. COM(2021)0206 – C9-0146/2021 – 2021/0106(COD) dostupný na https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_SK.html

⁸ V rámci pracovného stretnutia k príprave Štúdie, ktoré sa uskutočnilo dňa 11. decembra 2023.

1.1.1. Aktuálny stav legislatívy na úrovni EÚ v oblasti regulácie systémov umelej inteligencie

V súčasnosti je oblasť umelej inteligencie na úrovni EÚ regulovaná iba v rámci presahov do iných odvetví (napr. povinnosť súladu s GDPR⁹ pri spracúvaní osobných údajov s použitím systémov umelej inteligencie alebo povinnosť súladu s predpismi o všeobecnej bezpečnosti výrobkov, ak je systém umelej inteligencie komponentom určitého výrobku), avšak legislatívny rámec EÚ doposiaľ komplexne neupravoval vývoj, nasadenie a používanie systémov umelej inteligencie.

Prvou zásadnou legislatívnou iniciatívou EÚ, ktorej cieľom je komplexne regulovať používanie systémov umelej inteligencie je pripravované Nariadenie, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie.

Návrh Nariadenia je súčasťou stratégie „Formovanie digitálnej budúcnosti Európy“, bol predložený Komisiou Európskemu parlamentu dňa 21. apríla 2021 a predstavuje kľúčový krok EÚ v reakcii na rýchlo sa rozvíjajúcu oblasť umelej inteligencie. Nariadenie je výsledkom mnohých iniciatív a záväzkov na úrovni EÚ. Hlavným impulzom bol politický záväzok predsedníčky Komisie Ursuly von der Leyenovej, ktorá v rámci svojich politických usmernení na roky 2019 – 2024 oznámila zámer Komisie predložiť právne predpisy pre koordinovaný európsky prístup k ľudským a etickým dôsledkom AI. Toto vyhlásenie viedlo k publikácii bielej knihy o AI vo februári 2020, ktorá načrtla politické možnosti pre podporu rozvoja AI a riešenie s ním spojených rizík a následne k ďalším iniciatívnym krokom predchádzajúcim návrhu Nariadenia.

Okrem iných regulačných nástrojov Nariadenie zavádza povinnosť SR, zriadiť verejným orgánom kontrolovaný sandbox (alebo viacero sandboxov), ktorého cieľom má byť uľahčiť bezpečný vývoj, testovanie a validáciu inovatívnych systémov umelej inteligencie na obmedzený čas pred ich uvedením na trh alebo do prevádzky podľa konkrétneho plánu pod regulačným dohľadom, a ktorého uskutočniteľnosť v prostredí SR je predmetom tejto Štúdie. V čase prípravy tejto Štúdie nebolo zrejmé, či vyššie uvedená povinnosť nebude nahradená len možnosťou členských štátov zriadiť sandbox pre umelú inteligenciu. Bez ohľadu na uvedené, Štúdia hodnotí uskutočniteľnosť AI sandboxu v prostredí SR vo všeobecnosti bez ohľadu na to, či zriadenie sandboxu na úrovni SR bude povinné alebo dobrovoľné, pričom predmetom Štúdie je záujem zmapovať uskutočniteľnosť sandboxu pre umelú inteligenciu pri každej z daných alternatív.

So zavedením sandboxu resp. sandboxov pre oblasť umelej inteligencie však počítá APDTS - Akčný plán digitálnej transformácie Slovenska na roky 2023 – 2026, schválený vládou SR dňa 14. decembra 2022. Tento dokument definuje ciele SR v oblasti digitalizácie, pričom vymedzuje jednotlivé stratégie vrátane orgánov zodpovedných za ich realizáciu.

⁹ Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov) (ďalej len „GDPR“)

Súčasťou APDTS je v bode 3.1.1.7 aj opatrenie na vytvorenie experimentálnych regulačných prostredí (sandboxov) pre AI. Ako gestor zodpovedný za realizáciu tohto opatrenia je určené MIRRI (z iniciatívy ktorého bola vypracovaná Štúdia), pričom Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej len „**MIRRI**“) je určené aj ako gestor pre celú oblasť resp. ďalšie opatrenia týkajúce sa umelej inteligencie. MIRRI je v zmysle Kompetenčného zákona¹⁰ ústredný orgán určený pre oblasť investícií v rozsahu strategického plánovania a strategického projektového riadenia, ako aj koordináciu investičných projektov a vypracovanie národného strategického investičného rámca v pôsobnosti MIRRI, a vnútroštátnu implementáciu Agendy 2030.

Nariadenie je doplnené návrhom Smernice o zodpovednosti¹¹. Smernica o zodpovednosti je navrhnutá tak, aby doplnila Nariadenie, poskytujúc regulačný rámec pre otázky zodpovednosti a náhrady škody spojenej s používaním systémov umelej inteligencie. Jej cieľom je zabezpečiť, aby obeť škôd spôsobených systémami umelej inteligencie mali možnosť domôcť sa adekvátnej kompenzácie (pre bližšie informácie viď časť 1.2.1 Štúdie nižšie).

Okrem vyššie uvedeného na úrovni EÚ prebieha viacero ďalších iniciatív v oblasti regulácie AI, vrátane (i) návrhu súboru štandardných zmluvných doložiek pre obstarávanie vysokorizikových systémov umelej inteligencie, ktoré odrážajú požiadavky stanovené v Nariadení pre túto kategóriu systémov, a (ii) zapracovania úpravy pre vysokorizikové systémy umelej inteligencie do Návrhu Aktu o kybernetickej odolnosti¹² (pre bližšie informácie viď časť 1.3 Štúdie nižšie).

Nad rámec uvedeného, ešte uvádzame, že v oblasti umelej inteligencie prebieha iniciatíva Komisie ohľadom kreovania tzv. Paktu o umelej inteligencii (ďalej len „**Pakt**“). Jeho účelom je okrem iného preklenúť prechodné obdobie pred nadobudnutím účinnosti Nariadenia a zvýšiť dôveryhodnosť nových technológií. V rámci Paktu Spoločenosti majú možnosť dať dobrovoľný prísľub k dodržiavaniu povinností vyplývajúcich z Nariadenia spolu s opisom konkrétnych opatrení, ktoré už vykonávajú alebo plánujú zaviesť pre zabezpečenie súladu s Nariadením.¹³

1.1.2. Stručné zhrnutie základných aspektov navrhovaného Nariadenia relevantných pre implementáciu sandboxov

Primárnym cieľom Nariadenia (v znení, ktoré je reflektované v rámci Štúdie – viď vyššie) je zabezpečiť, že technológia umelej inteligencie bude využívaná spôsobom, ktorý je bezpečný, transparentný a etický, a že bude rešpektovať základné práva a slobody jednotlivcov. Nariadenie preto rozlišuje systémy umelej inteligencie na základe úrovne rizika, ktoré predstavujú pre základné ľudské práva a slobody, a zavádza príslušné regulačné požiadavky a povinnosti pre každú kategóriu. Hlavnou kategóriou systémov umelej inteligencie, na ktorú sa vzťahujú požiadavky Nariadenia sú tzv. vysokorizikové systémy umelej inteligencie (viď časť 1.1.1.4 nižšie).

¹⁰ Zákon č. 575/2001 Z. z., o organizácii činnosti vlády a organizácii ústrednej štátnej správy v znení neskorších predpisov (ďalej len „**Kompetenčný zákon**“).

¹¹ Návrh Smernice Európskeho parlamentu a Rady o prispôbení pravidiel mimozmluvnej občianskoprávnej zodpovednosti umelej inteligencii (smernica o zodpovednosti za umelú inteligenciu) COM/2022/496 (ďalej len „**Smernica o zodpovednosti**“).

¹² Návrh Nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020 COM(2022) 454 final (ďalej len „**Návrh Aktu o kybernetickej odolnosti**“).

¹³ Viď napr. <https://digital-strategy.ec.europa.eu/en/policies/ai-pact>

Okrem vyššie uvedeného, je cieľom Nariadenia aj podpora inovácií a konkurencieschopnosti v AI sektore, avšak súčasne so zabezpečením ochrany používateľov a prevencie potenciálnych škôd. Jedným z nástrojov pre dosiahnutie tohto cieľa je sú tzv. sandboxy pre umelú inteligenciu, ktoré poskytujú bezpečné a regulované prostredie, v ktorom môžu vývojári a firmy testovať nové aplikácie a systémy AI pod dohľadom regulačného orgánu. Tento prístup umožňuje potencionálnym poskytovateľom systémov umelej inteligencie experimentovať a rýchlo sa učiť z reálnych skúseností, zatiaľ čo minimalizuje riziká pre používateľov a širšiu spoločnosť. Sandboxy tak vytvárajú priestor pre inovácie, pričom je zároveň zachovaný dôraz na ochranu a bezpečnosť, čo je nevyhnutné pre budovanie dôvery verejnosti v technológiu AI.

Pre zabezpečenie vyššie uvedených cieľov Nariadenie kladie na členské štáty EÚ, vrátane SR, aj povinnosť zaviesť širšie inštitucionálne a regulačné štruktúry a mechanizmy potrebné pre efektívnu implementáciu a dohľad nad povinnosťami vyplývajúcimi z Nariadenia, a to v časovom rámci a v rozsahu predpokladanom Nariadením. Hlavné aspekty Nariadenia v rozsahu relevantnom pre Štúdiu uvádzame v nasledovných častiach.

1.1.2.1 Nariadenie – hlavné časové aspekty (míľniky)



Odišne od všeobecného režimu začiatku uplatňovania Nariadenia sa majú uplatňovať: (i) ustanovenia ktoré sa týkajú zriadenia inštitucionálneho rámca (t.j. notifikujúce a notifikované osoby, ustanovenia o Európskej rade pre umelú inteligenciu a určení príslušných vnútroštátnych orgánov), ktoré sa majú uplatňovať 3 mesiace od nadobudnutia účinnosti Nariadenia (hlava III kapitola 4 a hlava VI Nariadenia), a (ii) článok 71 Nariadenia t.j. ustanovenia o sankciách sa uplatňujú 12 mesiacov po nadobudnutí účinnosti Nariadenia.

1.1.2.2 Základné pojmy Nariadenia:¹⁴

„systém umelej inteligencie“	je strojový systém, ktorý je navrhnutý tak, aby fungoval s rôznymi úrovňami autonómie, a ktorý môže pre explicitné alebo implicitné ciele vytvárať výstupy, ako sú predpovede, odporúčania alebo rozhodnutia, ktoré ovplyvňujú fyzické alebo virtuálne prostredie (čl. 3 ods.1 bod 1 Nariadenia);
„vysokorizikový systém umelej inteligencie“	viď časť (iv) nižšie (Čl. 6 ods.1 a ods. 2 Nariadenia);
„riziko“	je kombinácia pravdepodobnosti výskytu ujmy a závažnosti tejto ujmy (Čl. 3 ods.1 bod 1a Nariadenia);
„významné riziko“	je riziko, ktoré je významné v dôsledku kombinácie jeho závažnosti, intenzity, pravdepodobnosti výskytu a trvania jeho účinkov a jeho schopnosti ovplyvniť jednotlivca, značný počet osôb alebo ovplyvniť konkrétnu skupinu osôb (čl. 3 ods.1 bod 1b Nariadenia);
„experimentálne regulačné prostredie“	je kontrolované prostredie vytvorené verejným orgánom, ktoré uľahčuje bezpečný vývoj, testovanie a validáciu inovatívnych systémov umelej inteligencie na obmedzený čas pred ich uvedením na trh alebo do prevádzky podľa konkrétneho plánu pod regulačným dohľadom (čl. 3 ods.1 bod 44g Nariadenia);
„nasadzujúci subjekt“	je každá fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý používa systém umelej inteligencie v rámci svojej právomoci, s výnimkou prípadov, keď sa systém umelej inteligencie používa v rámci osobnej neprofesionálnej činnosti (čl. 3 ods.1 bod 4 Nariadenia);
„poskytovateľ“	je fyzická alebo právnická osoba, orgán verejnej moci, agentúra alebo iný subjekt, ktorý vyvíja systém umelej inteligencie alebo ktorý má systém umelej inteligencie vyvinutý s cieľom uviesť ho na trh alebo do prevádzky pod vlastným menom alebo ochrannou známkou, či už za odplatu alebo bezodplatne (čl. 3 ods.1 bod 2 Nariadenia);
„prevádzkovateľ“	je poskytovateľ, nasadzujúci subjekt, splnomocnený zástupca, dovozca a distribútor (čl. 3 ods.1 bod 8 Nariadenia);
„dotknutá osoba“	je akákoľvek fyzická osoba alebo skupina osôb, na ktorú sa vzťahuje systém umelej inteligencie alebo ktorá je ním inak ovplyvnená (čl. 3 ods.1 bod 8a Nariadenia);
„distribútor“	je každá fyzická alebo právnická osoba v dodávateľskom reťazci okrem poskytovateľa alebo dovozcu, ktorá na trhu EÚ sprístupňuje systém umelej inteligencie bez toho, aby ovplyvňovala jeho vlastnosti (čl. 3 ods.1 bod 7 Nariadenia);
„dovozca“	je každá fyzická alebo právnická osoba usadená v EÚ, ktorá uvádza na trh alebo do prevádzky systém umelej inteligencie, ktorý je označený menom alebo ochrannou známkou fyzickej alebo právnickej osoby usadenej mimo Únie (čl. 3 ods.1 bod 6 Nariadenia);
„splnomocnený zástupca“	poskytovatelia usadení mimo Únie pred sprístupnením svojich systémov na trhu Únie písomným splnomocnením vymenujú splnomocneného zástupcu usadeného v EÚ (čl. 3 ods.1 bod 5 Nariadenia);
„uvedenie na trh“	je prvé sprístupnenie systému umelej inteligencie na trhu EÚ (čl. 3 ods.1 bod 9 Nariadenia);
„sprístupnenie na trh“	je každá dodávka systému umelej inteligencie na účely distribúcie alebo používania na trhu EÚ v rámci obchodnej činnosti, či už za odplatu, alebo bezodplatne (čl. 3 ods. 1 bod 10 Nariadenia);

¹⁴ V znení, ktoré je reflektované v rámci Štúdie (viď vyššie) - to sa aplikuje aj vo vzťahu k nasledovným sekciám Štúdie.

„ uviedenie do prevádzky “	je dodanie systému umelej inteligencie na prvé použitie priamo nasadzujúcemu subjektu alebo na vlastné použitie na trhu EÚ na zamýšľaný účel (čl. 3 ods. 1 bod 11 Nariadenia);
„ bezpečnostný komponent výrobku alebo systému “	je v súlade s harmonizačnými právnymi predpismi EÚ uvedenými v prílohe II Nariadenia komponent výrobku alebo systému, ktorý pre daný výrobok alebo systém plní bezpečnostnú funkciu alebo ktorého zlyhanie alebo porucha ohrozuje zdravie a bezpečnosť osôb (čl. 3 ods. 1 bod 14 Nariadenia).

Pre základné pojmy súvisiace s inštitucionálnym rámcom predpokladaným Nariadením vid' časť 2.1.1 Štúdie nižšie.

1.1.2.3 Základný rozsah pôsobnosti Nariadenia

Nariadenie sa vzťahuje na:

- poskytovateľov systémov umelej inteligencie, ktorí uvádzajú systémy umelej inteligencie na trh alebo do prevádzky v EÚ, bez ohľadu na to, či sú usadení v EÚ alebo v tretej krajine alebo uvádzajú na trh alebo do prevádzky systémy umelej inteligencie, ktoré spadajú medzi zakázané praktiky v zmysle Nariadenia¹⁵ mimo EÚ, ak sa poskytovateľ alebo distribútor takýchto systémov nachádza v EÚ;
- nasadzujúce subjekty systémov umelej inteligencie, ktoré majú miesto usadenia alebo ktoré sa nachádzajú v EÚ alebo v tretej krajine, v ktorej sa na základe medzinárodného práva verejného uplatňuje právo ktoréhokoľvek členského štátu EÚ alebo v ktorej sa výstup vytvorený systémom má používať v EÚ;
- dovozcov a distribútorov systémov umelej inteligencie, ako aj splnomocnených zástupcov poskytovateľov, ktorí majú svoje sídlo alebo sa nachádzajú v Únii.
- dotknuté osoby, ak sa nachádzajú v EÚ a ktorých zdravie, bezpečnosť alebo základné práva sú nepriaznivo ovplyvnené používaním systému umelej inteligencie, ktorý sa uvádza na trh alebo do prevádzky v EÚ.

Nariadenie sa nevzťahuje na (vid' čl. 2 Nariadenia):

- systémy umelej inteligencie vyvinuté alebo používané výlučne na vojenské účely;
- (i) výskumnú, testovaciu alebo vývojovú činnosť pred uvedením systému AI na trh alebo do prevádzky, ak sa tieto činnosti uskutočňujú v súlade so základnými právami a uplatniteľným právom Európskej Únie, pričom táto výnimka sa nevzťahuje na testovanie v reálnych podmienkach, a na (ii) systémy na základe bezplatných licencií (pokiaľ nie sú vysokorizikové alebo nespádajú pod zakázané praktiky);
- orgány verejnej moci v tretej krajine a medzinárodné organizácie, ktoré by inak spadali do pôsobnosti Nariadenia ale systémy umelej inteligencie používajú na základe medzinárodných dohôd, justičnej spolupráce alebo rozhodnutí Komisie o primeranosti.

¹⁵ Napr. systémy umelej inteligencie, ktoré využívajú ktorúkoľvek zo zraniteľností osoby alebo konkrétnej skupiny osôb.

1.1.2.4 Klasifikácia systémov umelej inteligencie

Nariadenie klasifikuje systémy umelej inteligencie podľa úrovne rizika, ktoré predstavujú. Táto klasifikácia umožňuje rôzne úrovne regulácie a dohľadu v závislosti od potenciálneho vplyvu príslušného systému umelej inteligencie na užívateľov a spoločnosť. Systémy s vyšším rizikom podliehajú prísnejším regulačným požiadavkám, zatiaľ čo tie s nižším rizikom majú menej prísne pravidlá.

Vzhľadom ku kontextu Štúdie uvádzame na tomto mieste stručne informácie iba k vysokorizikovým systémom umelej inteligencie, pričom Nariadenie (v znení návrhu reflektovaného v Štúdii) vo všeobecnosti za vysokorizikové považuje nasledovné systémy AI:¹⁶

- systém kumulatívne spĺňajúci nasledovné podmienky podľa článku 6 ods. 1 Nariadenia: (i) systém umelej inteligencie je určený na používanie ako bezpečnostný komponent výrobku, na ktorý sa vzťahujú harmonizačné právne predpisy EÚ uvedené v prílohe II Nariadenia¹⁷ (patria sem okrem iného hračky, výrobky pre letecký priemysel, autá, zdravotnícke pomôcky a výtahy), alebo je sám osebe takýmto výrobkom; a (ii) výrobok, ktorého bezpečnostným komponentom je systém umelej inteligencie, alebo samotný systém umelej inteligencie ako výrobok sa musí podrobiť posúdeniu zhody treťou stranou v súvislosti s rizikami pre zdravie a bezpečnosť s cieľom uviesť daný výrobok na trh alebo do prevádzky podľa harmonizačných právnych predpisov EÚ uvedených v prílohe II Nariadenia;
- systémy v zmysle článku 6 ods. 2 Nariadenia patriace do nasledovných samostatných oblastí regulovaných právom EÚ (v zmysle prílohy III Nariadenia), ak predstavujú významné riziko poškodenia zdravia, bezpečnosti alebo základných práv fyzických osôb: (i) biometrická identifikácia a kategorizácia FO, (ii) riadenie a prevádzka kritickej infraštruktúry, (iii) vzdelávanie a odborná príprava, (iv) zamestnanosť a riadenie pracovníkov a prístup k samostatnej zárobkovej činnosti, (v) prístup k základným službám (vrátane finančných) a ich využívanie, (vi) presadzovanie práva, (vii) riadenie migrácie, azylu a kontroly hraníc, a (viii) pomoc pri právnom výklade a uplatňovaní práva.

Pre vysokorizikové systémy umelej inteligencie Nariadenie vyžaduje okrem iného súlad s viacerými požiadavkami definovanými Nariadením ako napr. zavedenie trvalého procesu riadenia rizík, vypracovanie a pravidelnú aktualizáciu technickej dokumentácie a záznamov o operáciách, zabezpečenie transparentnosti vrátane plnenia povinností poskytovania informácií o systéme a jeho prevádzkovateľovi, ľudský dohľad pre zníženie rizík a plnenie ďalších povinností v zmysle Nariadenia.

Navyše sa musia tieto systémy pred uvedením na trh alebo do prevádzky podrobiť príslušnému postupu posudzovania zhody a udržiavať konzistentnú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti po celú dobu ich životného cyklu.

¹⁶ Rozsah definície vysokorizikových systémov (ako aj zavedenie možných výnimiek) bol jedným z hlavných bodov rokovaní o finálnom znení Nariadenia a kategorizácia systému ako vysokorizikového (so zohľadnením finálneho znenia Nariadenia) bude musieť byť osobitne zohľadňovaná v kontexte nastavenia fungovania pravidiel posudzovania zhody v rámci AI sandboxu s prihliadnutím na osobitné kritériá, ktoré sa na dané systémy vzťahujú.

¹⁷ Napr. smernica Európskeho parlamentu a Rady 2006/42/ES zo 17. mája 2006 o strojových zariadeniach (ďalej len „**Smernica o strojových zariadeniach**“), smernica Európskeho parlamentu a Rady 2009/48/ES z 18. júna 2009 o bezpečnosti hračiek (ďalej len „**Smernica o bezpečnosti hračiek**“), smernica Európskeho parlamentu a Rady 2013/53/EÚ z 20. novembra 2013 o rekreačných plavidlách a vodných skútroch a ďalšie vid'. Príloha II Nariadenia.

1.1.3. Základné povinnosti pre SR ako členský štát – najmä nastavenie inštitucionálneho rámca pre reguláciu, certifikáciu a dohľad nad trhom a zavedenie sandboxov pre umelú inteligenciu

V tejto časti Štúdie uvádzame stručné zhrnutie kľúčových povinností, ktoré Nariadenie ukladá členským štátom EÚ, vrátane Slovenskej republiky, a ktoré priamo alebo nepriamo súvisia so zriaďovaním sandboxov pre umelú inteligenciu (detailnejšia analýza vo vzťahu k inštitucionálnemu rámcu je zahrnutá v rámci časti 2.1 Štúdie nižšie):

- **vytvorenie národného inštitucionálneho rámca pre uplatňovanie Nariadenia** – Slovenská republika je v zmysle Nariadenia povinná zabezpečiť fungovanie inštitucionálneho rámca pre uplatňovanie Nariadenia buď zriadením nových orgánov s kompetenciami predpokladanými Nariadením a/alebo rozšírením kompetencií existujúcich orgánov – v tejto súvislosti vid' najmä časť 2.1.1 Štúdie nižšie (Tabuľka č. 1), ktorá obsahuje prehľad základných orgánov zodpovedných za uplatňovanie Nariadenia s prehľadom ich relevancie vo vzťahu k zriaďovaniu a fungovaniu sandboxov (najmä vnútroštátny dozorný orgán a zriaďujúci orgán).

Stručný prehľad OVM Slovenskej republiky dotknutých požiadavkami Nariadenia v kontexte zriaďovania sandboxu pre umelú inteligenciu je uvedený v časti 2.1.2 Štúdie nižšie, avšak s prihliadnutím na to, že definovanie inštitucionálneho ako aj legislatívneho rámca v oblasti regulácie umelej inteligencie v SR je aj predmetom TSI Analýzy¹⁸ a bude predmetom ďalších iniciatívnych krokov a rokovaní na strane relevantných OVM SR, ako aj s prihliadnutím na dodatočné upresnenia hlavných oblastí zamerania Štúdie zo strany MIRRI¹⁹, táto problematika nie je hĺbkovo analyzovaná v rámci tejto Štúdie;

- **vytvorenie legislatívneho rámca pre uplatňovanie Nariadenia** – bez ohľadu na priamu aplikovateľnosť Nariadenia, Slovenská republika bude v zmysle Nariadenia povinná prijať a/alebo upraviť príslušné národné právne predpisy v záujme zabezpečenia implementácie splnenia povinností vyplývajúcich z Nariadenia, vrátane, no bez obmedzenia, zákonov súvisiacich s určením vnútroštátneho **dozorného** orgánu a alokovaním právomocí v zmysle Nariadenia (vrátane dohľadových a sankčných právomocí a preferovane (ako bude uvedené nižšie) aj základného zákonného rámca pre fungovanie sandboxu pre umelú inteligenciu formou tzv. doložiek o experimentálnom režime)²⁰.

Rovnako ako aj v prípade povinností súvisiacich s implementáciou inštitucionálneho rámca predpokladaného Nariadením, nie je analýza požiadaviek na úpravu existujúcej legislatívy predmetom tejto Štúdie. Legislatívno-technické východiská a odporúčania v súvislosti so zriaďovaním a fungovaním sandboxu resp. sandboxov v rámci SR sú však uvedené v častiach 3.1.3.1 a 3.3 Štúdie nižšie;

- **zriadenie sandboxu** – povinnosť (a/alebo možnosť - vid' vyššie) zriadiť jeden alebo viacero sandboxov samostatne alebo v spolupráci s iným členským štátom resp. štátmi v súlade s požiadavkami Nariadenia, ktorý musí byť funkčný najneskôr v deň začatia uplatňovania Nariadenia

¹⁸ Dokument „Zlepšenie podmienok pre eGovernment a AI riešenia a podpora implementácie RRP na Slovensku“ vypracovaný v rámci Nástroja technickej podpory, v zmysle zmluvy o poskytnutí služieb č. REFORM/SC2022/13 (ďalej len „**TSI Analýza**“). V čase prípravy Štúdie nebola TSI Analýza sprístupnená, a tak neboli jej závery v rámci Štúdie reflektované.

¹⁹ Okrem iného na koordinačnom stretnutí dňa 22. novembra 2023.

²⁰ Vid' najmä časť 3.1.3.1 Štúdie.

(t.j. do dvoch rokov od nadobudnutia účinnosti Nariadenia) a prideliť dostatočné zdroje na zabezpečenie účinného a včasného súladu s touto požiadavkou (viď najmä časť 5.6 nižšie).

Ako už bolo uvedené vyššie, pre účely tejto Štúdie vychádzame z predpokladu (ktorý bol potvrdený v rámci komunikácie s MIRRI), že v podmienkach Slovenskej republiky dôjde k zriadeniu samostatného AI sandboxu potreby slovenského trhu, pričom tento prístup môže umožniť pružnejšie a komplexnejšie reagovať na špecifiká lokálneho prostredia a zabezpečiť plnú kontrolu a väčšiu flexibilitu procesu zriaďovania a fungovania sandboxu v porovnaní s potrebou zohľadňovania politických a regulačných špecifik iných jurisdikcií (v prípade alternatívy zriaďovania AI sandboxu v spolupráci s iným štátom). Rovnako s prihliadnutím na organizačno-technické, nákladové hľadiská, ako aj legislatívno-technické hľadiská, v rámci tejto Štúdie vychádzame z predpokladu (ktorý bol taktiež potvrdený v rámci komunikácie s MIRRI)²¹, že v oblasti AI by malo v prvej fáze dôjsť k zriadeniu jedného experimentálneho regulačného prostredia v rámci SR, na ktorého činnosti však budú môcť participovať aj ďalšie OVM v rozsahu ich (najmä) metodických a dohľadových právomocí.

1.2. Pravidlá EÚ na riešenie otázok zodpovednosti v súvislosti s novými technológiami vrátane systémov umelej inteligencie

Ako už bolo uvedené vyššie všeobecný regulačný rámec Nariadenia je doplnený návrhom Smernice o zodpovednosti, ktorá nateraz predstavuje hlavnú legislatívnu iniciatívu EÚ (okrem Nariadenia) v oblasti špecifického riešenia zodpovednosti súvisiacej s používaním systémov umelej inteligencie (nad rámec existujúcich predpisov v oblasti všeobecnej zodpovednosti za škodu - v tejto súvislosti viď najmä časť 3.1 Štúdie, vo vzťahu k existujúcemu zodpovednostnému režimu v rámci SR).²² Keďže v aktuálnom stave Smernica o zodpovednosti nie je špecificky relevantná vo vzťahu k analýze možnosti zriadiť sandbox pre umelú inteligenciu v rámci SR, nie je v rámci Štúdie bližšie analyzovaná.

1.2.1. Hlavné ciele a riešenia predpokladané Smernicou o zodpovednosti

Smernica o zodpovednosti sleduje nasledovné hlavné ciele: (i) ochrana dotknutých osôb, resp. ochrana slabšej strany (poškodeného); a (ii) odstránenie neistoty pre subjekty, ktoré vyvíjajú systémy umelej inteligencie a vytýčenie hraníc ich zodpovednosti.

Medzi hlavné riešenia na dosiahnutie vyššie uvedených cieľov, ktoré prináša Smernica o zodpovednosti patrí:

- **zavedenie zjednodušeného režimu pre získanie dôkazov** – na žiadosť žalobcu/používateľa môže súd vydať príkaz na poskytnutie dôkazov, ktoré sú k dispozícii o konkrétnom vysokorizikovom systéme umelej inteligencie, ktorý údajne zavinil škodu; ak žalovaný nesplní príkaz súdu v rámci nároku na náhradu škody a neposkytne alebo nezachová dôkazy, ktoré má k dispozícii, súd bude predpokladať, že žalovaný si nesplnil príslušnú povinnosť náležitej starostlivosti (viď nižšie);

²¹ Okrem iného na koordinačnom stretnutí dňa 22. novembra 2023.

²² Pre účely Štúdie vychádzame zo znenia návrhu Smernice o zodpovednosti zo dňa 28. septembra 2022 č. 2022/0303 (COD).

- **zavedenie vyvrátiteľnej domnienky príčinnej súvislosti medzi pochybením žalovaného a výstupom alebo nevytvorením výstupu systému umelej inteligencie** za predpokladu splnenia nasledovných podmienok: (i) preukázanie alebo predpoklad nedodržania náležitej starostlivosti (poškodená osoba nemusí preukazovať porušenie príslušných povinností, ale stačí porušenie náležitej starostlivosti); (ii) je dostatočne pravdepodobné, že pochybenie systému ovplyvnilo výstup zo systému AI alebo jeho nevytvorenie (postačuje dostatočná pravdepodobnosť); a (iii) navrhovateľ preukáže, že výstup AI systému (alebo jeho nevytvorenie) spôsobil vznik škody.

1.2.2. Časový rámec a povinnosti členských štátov EÚ

Príprava a prijatia finálneho návrhu Nariadenia spomalili rokovania o Smernici o zodpovednosti, pričom v súčasnej dobe nie je známy konkrétny časový odhad, kedy by Smernica o zodpovednosti mohla byť prijatá. V dostupnom návrhu Smernice o zodpovednosti je stanovená transpozičná lehota 2 roky od nadobudnutia jej účinnosti.

V súvislosti s implementáciou požiadaviek Smernice o zodpovednosti bude Slovenská republika povinná zabezpečiť včasnú implementáciu inštitútov predpokladaných Smernicou o zodpovednosti (vrátane tých sumarizovaných vyššie) do slovenského právneho poriadku v rámci stanovenej transpozičnej lehoty.

1.3. Prehľad základných sektorových bezpečnostných právnych predpisov relevantných v kontexte Nariadenia a zriaďovania sandboxov - môže podliehať ďalšej úprave

Na systémy umelej inteligencie sa aplikuje resp. bude aplikovať široká škála existujúcich a pripravovaných bezpečnostných predpisov EÚ, vrátane predpisov týkajúcich sa ochrany osobných údajov a bezpečnostných požiadaviek na výrobky a najmä tých, do ktorých môžu byť zakomponované systémy AI.

V kontexte Nariadenia²³ a špecificky problematiky zriaďovania a fungovania sandboxov budú relevantné najmä predpisy stanovujúce bezpečnostné požiadavky, ktoré bude potrebné zohľadňovať v rámci prevádzky sandboxu, tak z pohľadu identifikácie a mitigácie bezpečnostných rizík v priebehu testovania, ako aj pre účely zabezpečenia zhody s požiadavkami Nariadenia a príslušnými osobitnými bezpečnostnými predpismi zo strany účastníkov sandboxu pred uvedením na trh. Ako bude uvedené nižšie (viď najmä časť 2.1.1 nižšie), Nariadenie predpokladá, že správy o výstupoch zo sandboxu budú zohľadňované tak notifikovanými osobami²⁴ ako aj príslušnými orgánmi dohľadu v kontexte postupov posudzovania zhody alebo kontrol v rámci dohľadu nad trhom.

²³ Nariadenie, okrem iného, v odôvodnení (2c) uvádza, že systémy umelej inteligencie v rámci EÚ podliehajú príslušným právnym predpisom o bezpečnosti výrobkov, ktoré poskytujú rámec na ochranu spotrebiteľov pred nebezpečnými výrobkami vo všeobecnosti, a takéto právne predpisy by sa mali naďalej uplatňovať. Nariadením nie sú dotknuté ani pravidlá stanovené v iných právnych aktoch EÚ týkajúcich sa ochrany spotrebiteľa a bezpečnosti výrobkov vrátane nariadenia (EÚ) 2017/2394 o spolupráci medzi národnými orgánmi zodpovednými za presadzovanie právnych predpisov na ochranu spotrebiteľa, nariadenia (EÚ) 2019/1020 o dohľade nad trhom a súlade výrobkov (ďalej len „Nariadenie 2019/1020“), smernice 2001/95/ES o všeobecnej bezpečnosti výrobkov a smernice 2013/11/EÚ o alternatívnom riešení spotrebiteľských sporov.

²⁴ Viď Tabuľka č. 1 Prehľad inštitucionálneho rámca predpokladaného Nariadením vo vzťahu k zriaďovaniu a fungovaniu sandboxov.

Nižšie uvádzame prehľad vybraných platných a pripravovaných bezpečnostných predpisov EÚ (resp. ich okruhov), ktoré v súvislosti s predmetom Štúdie považujeme za najrelevantnejšie:

- **Všeobecné nariadenie o ochrane osobných údajov (GDPR)** – GDPR ako všeobecný predpis upravujúci podmienky spracúvania osobných údajov v rámci EÚ sa bude vzťahovať aj na systémy umelej inteligencie pokiaľ v akejkoľvek fáze ich vývoja alebo použitia dôjde k spracúvaniu osobných údajov. Vo vzťahu k spracúvaniu osobných údajov v rámci sandboxov, Nariadenie predpokladá v istej miere aj zapojenie Úradu na ochranu osobných údajov SR (ďalej len „ÚOOÚ“). Nariadenie vymedzuje aj osobitné podmienky spracúvania osobných údajov v rámci sandboxu, pričom požaduje, aby existovali účinné mechanizmy monitorovania umožňujúce zistiť, či počas experimentovania v sandboxe môžu vzniknúť vysoké riziká pre práva a slobody dotknutých osôb, ako sa uvádzajú v čl. 35 GDPR ako aj mechanizmus reakcie na rýchle zmiernenie týchto rizík a v prípade potreby na zastavenie spracúvania²⁵ (viď časť 3.1.2.2 Štúdie nižšie);
- **Nariadenie o všeobecnej bezpečnosti výrobkov**²⁶ – toto nariadenie sa uplatňuje na výrobky uvedené na trh alebo sprístupnené na trhu, pokiaľ podľa práva EÚ, ktoré upravuje bezpečnosť dotknutých výrobkov, neexistujú osobitné ustanovenia s rovnakým cieľom. Ak výrobky podliehajú osobitným požiadavkám na bezpečnosť stanoveným v práve EÚ (viď nižšie), toto nariadenie sa vzťahuje iba na tie aspekty a riziká alebo kategórie rizík, ktoré nie sú zahrnuté do týchto požiadaviek. Nariadenie o všeobecnej bezpečnosti výrobkov sa v príslušnom rozsahu môže vzťahovať aj na systémy umelej inteligencie pokiaľ sa používajú vo výrobkoch pre spotrebiteľov (okrem požiadaviek Nariadenia musia byť výrobky obsahujúce systémy AI klasifikované ako bezpečné podľa Nariadenia o všeobecnej bezpečnosti výrobkov);
- **Bezpečnostné predpisy tzv. Nového legislatívneho rámca** (v angl. New legislation framework)²⁷ – stanovujú harmonizované normy pre akreditáciu, posúdenie zhody, dohľad na trhom a označovanie určených výrobkov predávaných v EÚ, pričom tieto predpisy bude potrebné zohľadňovať v kontexte celkového posudzovania zhody daných výrobkov s príslušnými predpismi a Nariadením, ak ich komponentmi budú systémy AI²⁸ resp. v inom kontexte stanovenom Nariadením a danými predpismi (prípadne v znení ich zmien vyvolaných Nariadením). Obdobne budú relevantné aj sektorové bezpečnostné predpisy mimo Nový legislatívny rámec, najmä tzv. predpisy podľa starého prístupu (napr. letectvo²⁹, automobily), avšak len v rozsahu stanovenom Nariadením;

²⁵ Viď čl. 54 ods. 1 Nariadenia.

²⁶ Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/988 z 10. mája 2023 o všeobecnej bezpečnosti výrobkov, ktorým sa mení nariadenie Európskeho parlamentu a Rady (EÚ) č. 1025/2012 a smernica Európskeho parlamentu a Rady (EÚ) 2020/1828 a zrušuje smernica Európskeho parlamentu a Rady 2001/95/ES a smernica Rady 87/357/EHS (ďalej len „Nariadenie o všeobecnej bezpečnosti výrobkov“).

²⁷ Viď https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en

²⁸ Viď napr. Smernica o strojových zariadeniach; Smernica o bezpečnosti hračiek; smernica Európskeho parlamentu a Rady 2013/53/EÚ z 20. novembra 2013 o rekreačných plavidlách a vodných skútroch; Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/745 o zdravotníckych pomôckach, zmene smernice 2001/83/ES, nariadenia (ES) č. 178/2002 a nariadenia (ES) č. 1223/2009 a o zrušení smerníc Rady 90/385/EHS a 93/42/EHS.

²⁹ Viď napr. Nariadenie Európskeho parlamentu a Rady (ES) č. 300/2008 z 11. marca 2008 o spoločných pravidlách v oblasti bezpečnostnej ochrany civilného letectva a o zrušení nariadenia (ES) č. 2320/2002. NARIADENIE EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2023/1230 zo 14. júna 2023 o strojových zariadeniach a o zrušení smernice Európskeho parlamentu a Rady 2006/42/ES a smernice Rady 73/361/EHS

Pozn. v tejto súvislosti uvádzame, že Smernica o strojových zariadeniach (ako jeden z kľúčových nástrojov Nového legislatívneho rámca) bude s účinnosťou od 14. januára 2027 nahradená Nariadením o strojníckych výrobkoch³⁰ - aj keď toto nariadenie špecificky neodkazuje na Nariadenie, čiastočne rieši aj aspekty súvisiace so systémami umelej inteligencie vrátane zavedenia požiadavky, že systémy so samovyvíjajúcim sa správaním, ktoré zabezpečujú bezpečnostné funkcie, by sa mali zahrnúť do rámca produktov podliehajúcim posudzovaniu zhody v zmysle tohto nariadenia vzhľadom na ich vlastnosti, ako je závislosť od údajov, nepriehľadnosť, autonómnosť a prepojitelnosť, čo by mohlo výrazne zvýšiť pravdepodobnosť a závažnosť ujmy a vážne ovplyvniť bezpečnosť strojového zariadenia alebo súvisiaceho výrobku (ak však strojové zariadenie obsahuje systém, ktorého bezpečnostný komponent už bol podrobený posudzovaniu zhody treťou stranou, keď bol uvedený na trh nezávisle, toto strojové zariadenie by nemalo byť opätovne certifikované treťou stranou len na základe zabudovania tohto systému)³¹ (viď najmä odôvodnenia (54) a (55) Nariadenia o strojníckych výrobkoch);

- **Predpisy o kybernetickej bezpečnosti** – v zmysle Nariadenia sú požiadavky kybernetickej bezpečnosti medzi základnými aspektmi, ktoré je potrebné posudzovať vo vzťahu k systémom umelej inteligencie (a najmä vysokorizikovým systémom), vrátane v rámci prostredia AI sandboxov.

V tomto ohľade odkazujeme primárne na (i) Zákon o kybernetickej bezpečnosti³² a súvisiace predpisy v oblasti kybernetickej bezpečnosti (ako napr. DORA)³³, ktoré sa na systémy umelej inteligencie môžu vzťahovať, ak sú súčasťou informačného systému alebo služieb, na ktoré sa vzťahuje režim Zákona o kybernetickej bezpečnosti alebo súvisiacich predpisov.

Osobitne tiež poukazujeme na **Návrh Aktu o kybernetickej odolnosti**³⁴ – rovnako aj tento predpis je stále v legislatívnom procese (a tak je potrebné upozorniť na všeobecné riziko, že aktuálne znenie návrhu predpisu sa môže ďalej meniť a budúce nastavenie vzťahov k sandboxu pre umelú inteligenciu bude musieť zohľadňovať aktualizované znenie tohto predpisu)), pričom je zameraný na kybernetickú odolnosť produktov s digitálnymi prvkami vo všeobecnosti, nielen špecificky voči systémom AI. Podľa návrhu, ak vysokorizikové AI systémy vyhovujú základným požiadavkám Aktu o kybernetickej odolnosti, mali by byť považované za systémy spĺňajúce požiadavky kybernetickej bezpečnosti aj podľa Nariadenia. Pre hodnotenie zhody týchto vysokorizikových AI systémov by sa však mal spravidla uplatňovať režim Nariadenia.³⁵

³⁰ Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1230 zo 14. júna 2023 o strojových zariadeniach a o zrušení smernice Európskeho parlamentu a Rady 2006/42/ES a smernice Rady 73/361/EHS (ďalej len „**Nariadenie o strojníckych výrobkoch**“).

³¹ Rovnako ustanovenia Nariadenia o strojníckych výrobkoch týkajúce sa posudzovania zhody softvéru zaisťujúceho bezpečnostné funkcie treťou stranou stanovené v tomto nariadení by sa mali uplatňovať len na systémy s úplne alebo čiastočne sa samovyvíjajúcim správaním, ktoré využívajú prístupy strojového učenia zaisťujúce bezpečnostné funkcie.

³² Zákon č. 69/2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „**Zákon o kybernetickej bezpečnosti**“).

³³ Nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (DORA).

³⁴ Návrh Nariadenia Európskeho parlamentu a Rady o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadenia (EÚ) 2019/1020 COM(2022) 454 final.

³⁵ Viď odôvodnenie (29) Návrhu Aktu o kybernetickej odolnosti.

2 Analýza dotknutých subjektov na strane orgánov verejnej moci, regulovaných subjektov a ostatných zainteresovaných osôb vo vzťahu k implementácii sandboxu (experimentálneho regulačného prostredia) v prostredí Slovenskej republiky

V tejto časti Štúdie sa venujeme analýze dotknutých subjektov vo vzťahu k implementácii sandboxu pre umelú inteligenciu v prostredí Slovenskej republiky, pričom najmä (i) sumarizujeme základný inštitucionálny rámec predpokladaný Nariadením vo vzťahu k jeho uplatňovaniu vo všeobecnosti a špecificky vo vzťahu k zriaďovaniu sandboxov (časť 2.1.1 nižšie), (ii) identifikujeme OVM SR, ktoré budú zohrávať kľúčovú rolu pre zavádzanie AI sandboxu v prostredí SR (časť 2.1.2 Štúdie), (iii) poskytujeme prehľad o ďalších dotknutých osobách a ich úlohách pri zriaďovaní a fungovaní AI sandboxu (časť 2.1.2 a 2.2 Štúdie), a (iv) analyzujeme základné dopady zriadenia a fungovania AI sandboxu na právnické a fyzické osoby a hodnotíme, ako môže ovplyvniť aktérov a zúčastnené strany v kontexte slovenského právneho a ekonomického prostredia (časť 2.3 Štúdie).

2.1 Analýza orgánov verejnej moci v rámci SR, ktoré sú príslušné na implementovanie Nariadenia alebo ich spolupráca bude potrebná na zabezpečenie fungovania sandboxu

Ako bolo uvedené aj vyššie, s prihliadnutím na špecifikáciu zamerania Štúdie v zmysle požiadaviek MIRRI, pre účely tejto Štúdie poskytujeme stručný rámcový prehľad dotknutých OVM SR a iných subjektov v kontexte zriaďovania sandboxu v zmysle Nariadenia, pričom konkrétne nastavenie inštitucionálneho rámca predpokladaného Nariadením a s tým súvisiace dopady na príslušné OVM SR a iné subjekty bude závisieť od finálneho prístupu zvoleného SR zohľadňujúc okrem iného závery a odporúčania TSI Analýzy.

2.1.1. Prehľad inštitúcií, ktoré bude potrebné zriadiť a/alebo ktorých kompetencie bude potrebné alokovať existujúcim orgánom za účelom implementácie požiadaviek Nariadenia vo vzťahu k zriaďovaniu sandboxov

V súvislosti s definovaním OVM SR potenciálne dotknutých požiadavkami Nariadenia vo vzťahu k zriaďovaniu a fungovaniu sandboxov v prvom rade v Tabuľke č. 1 uvádzame základný prehľad inštitúcií, ktoré bude potrebné zriadiť a/alebo ktorých kompetencie bude potrebné alokovať existujúcim orgánom za účelom implementácie požiadaviek Nariadenia vo vzťahu k zriaďovaniu sandboxov

Tabuľka č.1 Prehľad inštitucionálneho rámca predpokladaného Nariadením vo vzťahu k zriaďovaniu a fungovaniu sandboxov

Inštitúcia	Základná definícia	Základné kompetencie	Poznámka ³⁶
Vnútroštátny dozorný orgán (čl. 3 ods. 1 bod 42 Nariadenia)	Verejný orgán, ktorý má byť poverený v rámci SR zodpovednosťou: - za vykonávanie a uplatňovanie Nariadenia; - za koordináciu činností zverených danému členskému štátu - za pôsobenie ako jednotné kontaktné miesto pre Komisiu - za zastupovanie členského štátu v riadiacej rade úradu pre umelú inteligenciu; SR má povinnosť určiť vnútorný dozorný orgán najneskôr do [troch mesiacov od nadobudnutia účinnosti Nariadenia]³⁷.	- uplatňovanie a vykonávanie Nariadenia; - pôsobnosť ako jednotné kontaktné miesto pre Nariadenie. - poskytovanie usmernení a poradenstva týkajúceho sa vykonávania Nariadenia, a to aj MSP a startupom; - pôsobnosť orgánu dohľadu nad trhom podľa Nariadenia s právomocami a povinnosťami ako orgány dohľadu nad trhom podľa Nariadenia 2019/1020 a v oblasti kontroly systémov umelej inteligencie na trhu EÚ; - koordinácia činnosti s inými príslušnými vnútroštátnymi orgánmi alebo subjektmi, ktoré vykonávajú dohľad nad uplatňovaním harmonizačného práva EÚ uvedeného v prílohe II Nariadenia alebo iného práva EÚ, ktoré by mohlo byť relevantné pre vysokorizikové systémy umelej inteligencie uvedené v prílohe III Nariadenia; - prijímanie opatrení pri incidentoch súvisiacich s vysokorizikovými systémami umelej inteligencie a vybavovanie sťažností FO; - oprávnenie udeľovať výnimky z povinnosti vykonať posúdenie zhody (čl. 47 Nariadenia); - spolupráca na európskej úrovni s ďalšími vnútroštátnymi dozornými orgánmi a v rámci Riadiacej rady Úradu	Organizačná štruktúra musí zabezpečiť objektivitu a nestrannosť a nezávislosť pri výkonne činnosti. S prihliadnutím na pôsobnosť v oblasti vydávania usmernení a poradenstva týkajúceho sa vykonávania Nariadenia (čl. 59 ods. 7 Nariadenia) a dohľadu a kontroly v oblasti pôsobnosti Nariadenia (čl. 59 ods. 2 Nariadenia) sa OVM, ktorý bude SR určený ako vnútroštátny dozorný orgán javí ako vhodný orgán, v ktorého gescii by malo byť zriadenie sandboxu (tj. mal by mať kompetencie „zriaďujúceho orgánu“), ak nebudú identifikované dôvody, pre ktoré by mal byť zriaďujúcim orgánom iný OVM SR.
Príslušný vnútroštátny orgán (čl. 3 ods. 1 bod 43 Nariadenia)	Ktorýkoľvek z vnútroštátnych OVM SR, ktoré budú zodpovedné za presadzovanie Nariadenia.		Pôjde najmä o OVM určený ako vnútroštátny dozorný orgán.
Ďalšie vnútroštátne orgány alebo príslušné orgány dohľadu a nápravy (čl. 53 ods. 2 a 3 Nariadenia)	OVM SR, ktoré sú zodpovedné za dohľad nad určitými sektorovými aspektmi systémov umelej inteligencie testovaných v rámci AI sandboxu, vrátane orgánov dohľadu nad trhom (viď nižšie).	Tieto orgány majú byť zapojené do prevádzky sandboxu a/alebo spolupracovať so zriaďujúcim orgánom pri dohľade nad prevádzkou sandboxu v plnom rozsahu svojich príslušných úloh a právomocí.	Pôjde najmä o OVM pôsobiace ako orgány dohľadu nad trhom a iné OVM s dohľadovou právomocou napr. ÚOOÚ vo vzťahu k systémom umelej inteligencie spracúvajúcim osobné údaje.

³⁶ Každý členský štát stanoví pravidlá pre správne pokuty ukladané orgánom verejnej moci a subjektom zriadeným v danom členskom štáte.

³⁷ Podľa informácií komunikovaných MIRRI na stretnutí dňa 11. decembra 2023 je možné, že táto povinnosť bude v lehote jedného roka odo dňa účinnosti Nariadenia.

Inštitúcia	Základná definícia	Základné kompetencie	Poznámka ³⁶
Zriaďujúci orgán (čl. 53 a nasl. Nariadenia)	Orgán SR zriaďujúci sandbox pre umelú inteligenciu v zmysle Nariadenia zodpovedný za zriadenie a fungovanie sandboxu v zmysle Nariadenia a za dosiahnutie jeho cieľov v zmysle čl. 53 ods. 1e Nariadenia	• zriaďiť a zabezpečiť prevádzku sandboxu v súlade s kritériami stanovenými v čl. 53a Nariadenia; • prideliť dostatočné zdroje na zriadenie AI sandboxu v zmysle Nariadenia; • poskytovanie usmernení a dohľadu v rámci AI sandboxu s cieľom identifikovať riziká, najmä pre základné práva, demokraciu a právny štát, zdravie a bezpečnosť a životné prostredie, testovať a preukazovať zmierňujúce opatrenia pre identifikované riziká a ich účinnosť a zabezpečiť súlad s požiadavkami Nariadenia a prípadne s inými právnymi predpismi EÚ a SR; • vypracovanie a poskytovanie správ o výstupoch z AI sandboxu orgánom dohľadu nad trhom alebo prípadne notifikovaným osobám, ktoré by mali byť zohľadňované v kontexte postupov posudzovania zhody alebo kontrol v rámci dohľadu nad trhom; • právomoc <u>neprijať</u> žiadne administratívne donucovacie opatrenia za porušenie Nariadenia ak potenciálni poskytovatelia dodržiavajú konkrétny plán dohodnutý so zriaďujúcim orgánom a podmienky svojej účasti a v dobrej viere sa riadia usmerneniami zriaďujúceho orgánu; • zabezpečiť, že pokiaľ inovačné systémy umelej inteligencie spracúvajú osobné údaje alebo na inom základe podliehajú dohľadu ďalších vnútroštátnych orgánov alebo príslušných orgánov, ktoré poskytujú alebo podporujú prístup k osobným údajom, aby tieto orgány boli zapojené do prevádzky sandboxu a do dohľadu nad jeho aspektmi v plnom rozsahu svojich príslušných úloh a právomocí; • spolupráca v rámci a poskytovanie informácií a správ Úradu; • zabezpečenie prístupu k sandboxu pre MSP a startupy bezplatne bez toho, aby boli dotknuté mimoriadne náklady, ktoré môže zriaďujúci orgán vymáhať spravodlivým a primeraným spôsobom;	Zriaďujúcim orgánom môže byť vnútroštátny dozorný orgán alebo iný OVM SR.

Inštitúcia	Základná definícia	Základné kompetencie	Poznámka ³⁸
Orgán dohľadu nad trhom (čl. 3 ods. 1 bod 26 Nariadenia)	Vnútroštátny orgán, ktorý vykonáva činnosti a prijíma opatrenia podľa Nariadenia 2019/1020, pričom orgánom dohľadu nad trhom pre účely Nariadenia je v zmysle Nariadenia vnútroštátny dozorný	Dohľadom nad trhom je činnosť a opatrenia na zabezpečenie toho, aby boli výrobky v súlade s požiadavkami stanovenými v uplatniteľných harmonizačných právnych predpisoch EÚ a zaručovali ochranu verejného záujmu, ktorého sa týkajú tieto právne predpisy. Kompetencie v zmysle Nariadenia:	V prostredí SR sú aktuálne orgánmi dohľadu nad trhom nasledovné orgány ³⁹ : • jednotným úradom pre spoluprácu je: Ministerstvo

³⁸ Každý členský štát stanoví pravidlá pre správne pokuty ukladané orgánom verejnej moci a subjektom zriadeným v danom členskom štáte.

³⁹ Čl. 3 ods. 1 bod. 26 Nariadenia - „orgán dohľadu nad trhom“ je vnútroštátny orgán, ktorý vykonáva činnosti a prijíma opatrenia podľa Nariadenia 2019/1020.

Inštitúcia	Základná definícia	Základné kompetencie	Poznámka ³⁸
	orgán s výnimkami uvedenými nižšie: V prípade vysokorizikových systémov umelej inteligencie súvisiacich s výrobkami, na ktoré sa vzťahujú právne akty uvedené v oddiele A prílohy II Nariadenia, je orgánom dohľadu nad trhom na účely tohto nariadenia orgán zodpovedný za činnosti dohľadu nad trhom určený podľa uvedených právnych aktov (v podmienkach SR najmä orgány uvedené v poznámkach k tomuto bodu). V prípade systémov umelej inteligencie, ktoré uvádzajú na trh, do prevádzky alebo používajú finančné inštitúcie regulované právnymi predpismi EÚ o finančných službách, je orgánom dohľadu nad trhom na účely Nariadenia príslušný orgán zodpovedný za finančný dohľad nad týmito inštitúciami v rámci SR - NBS. V prípade systémov umelej inteligencie, ktoré sa používajú na účely presadzovania práva, Nariadenie predpokladá určenie ÚOOÚ ako orgánu dohľadu nad trhom.	- dohľad nad trhom v zmysle čl. 63 a nasl. Nariadenia, vrátane vykonávania neohlásených kontrol vysokorizikových systémov umelej inteligencie na mieste a na diaľku a získavania vzoriek súvisiacich s vysokorizikovými systémami umelej inteligencie, a to aj prostredníctvom kontrol na diaľku, s cieľom vykonávať reverzné inžinierstvo systémov umelej inteligencie a získavať dôkazy na identifikovanie nesúladu; <u>zohľadňovanie správy o výstupoch (resp. výstupné správy) z AI sandboxu vypracovaných zriaďujúcim orgánom v kontexte kontrol v rámci dohľadu nad trhom.</u> Kompetencie v zmysle Nariadenia 2019/1020 (výber): - právomoc vyžadovať od hospodárskych subjektov poskytnúť prístup k relevantným dokumentom, technickým špecifikáciám, údajom alebo informáciám týkajúcim sa súladu a technických parametrov výrobku vrátane prístupu k zabudovanému softvéru; - právomoc požadovať od hospodárskych subjektov, aby poskytovali relevantné informácie o dodávateľskom reťazci, o podrobnostiach o distribučnej sieti, o množstvách výrobkov na trhu; a - právomoc vykonávať neohlásené kontroly na mieste a fyzické kontroly výrobkov.	hospodárstva SR (ďalej len „MH SR“); - Slovenská obchodná inšpekcia (ďalej len „SOI“); - Slovenská inšpekcia životného prostredia; - Štátny úrad pre kontrolu liečiv ďalej len „ŠUKL“; - Slovenský metrologický inšpektorát; - Úrad verejného zdravotníctva Slovenskej republiky; - Hlavný banský úrad; - Ústredný kontrolný a skúšobný ústav poľnohospodársky; - Inšpektoráty práce a Národný inšpektorát práce; - Ministerstvo dopravy Slovenskej republiky; - Dopravný úrad.
Notifikujúci orgán (čl. 3 ods. 1 bod 19 Nariadenia)	Vnútroštátny orgán, ktorý má byť v rámci SR poverený zodpovednosťou za: - stanovenie a vykonávanie nevyhnutných postupov na posudzovanie, určovanie a notifikáciu orgánov posudzovania zhody (viď nižšie); a - za ich monitorovanie. Pri zriadení/určení notifikujúceho orgánu nesmie dôjsť ku konfliktu	- stanovenie a výkon postupov nevyhnutných pre posúdenie, určenie a notifikáciu orgánov posudzovania zhody (notifikované osoby); - notifikujúce orgán notifikujú Komisiu a iné členské štáty iba o tých orgánoch posudzovania zhody, ktoré splnili požiadavky stanovené Nariadením (pozn. dotknutý orgán posudzovania zhody môže vykonávať činnosti notifikovanej osoby iba vtedy, ak Komisia ani ostatné členské štáty nevzniesli námietky v čase a spôsobom predpokladaným Nariadením); - monitorovanie orgánov posudzovania zhody (objektivita a nestrannosť výkonu	SR môže v zmysle čl. 30 ods. 2 Nariadenia ako notifikujúci orgán určiť vnútroštátny akreditačný orgán v zmysle Nariadenia 765/2008⁴⁰ t.j. Slovenskú národnú akreditačnú službu (ďalej len „SNAS“) (v zmysle Zákona o akreditácii alebo aj iný OVM.

⁴⁰ Nariadenie Európskeho parlamentu a Rady (ES) č. 765/2008 z 9. júla 2008, ktorým sa stanovujú požiadavky akreditácie a dohľadu nad trhom v súvislosti s uvádzaním výrobkov na trh a ktorým sa zrušuje nariadenie (EHS) č. 339/93

Inštitúcia	Základná definícia	Základné kompetencie	Poznámka ³⁸
	záujmov s orgánmi posudzovania zhody. Okrem iného, notifikujúce orgány <u>nesmú</u> ponúkať ani poskytovať žiadne činnosti, ktoré vykonávajú orgány posudzovania zhody, ani žiadne poradenské služby na komerčnom či konkurenčnom základe.	činnosti, predchádzanie konfliktu záujmov).	
Notifikovaná osoba (čl. 3 ods. 1 bod 22 Nariadenia)	Orgán posudzovania zhody (viď nižšie) určený v súlade s Nariadením a inými relevantnými harmonizačnými právnymi predpismi EÚ a notifikovaný Komisií/iným členským štátom spôsobom predpokladaným Nariadením. Na účely vykonávania postupu posudzovania zhody uvedeného v prílohe VII Nariadenia si poskytovateľ môže vybrať <u>ktorúkoľvek</u> z notifikovaných osôb.	- notifikované osoby overujú zhodu vysokorizikového systému umelej inteligencie v súlade s postupmi posudzovania zhody uvedenými v Nariadení a v rozsahu stanovenom Nariadením; - informačné povinnosti voči notifikujúcemu orgánu vo vzťahu k svojej činnosti (vydané certifikáty, zamietnuté žiadosti a pod...); <u>zohľadňovanie správ o výstupoch (resp. výstupné správy) z AI sandboxu vypracovaných zriaďujúcim orgánom v kontexte postupov posudzovania zhody.</u>	V prípade vysokorizikových systémov umelej inteligencie, na ktoré sa vzťahujú právne akty uvedené v oddiele A prílohy II Nariadenia, sa poskytovateľ má riadiť príslušným posúdením zhody vyžadovaným podľa uvedených právnych aktov. Na uvedené vysokorizikové systémy umelej inteligencie sa vzťahujú požiadavky stanovené v kapitole 2 hlavy III Nariadenia a musia byť zahrnuté do tohto posúdenia. Na účely uvedeného posúdenia sú notifikované osoby, ktoré boli notifikované podľa uvedených právnych aktov, oprávnené kontrolovať zhodu vysokorizikových systémov umelej inteligencie s požiadavkami stanovenými v kapitole 2 hlavy III Nariadenia za predpokladu, že v rámci postupu notifikácie podľa uvedených právnych aktov sa posúdil súlad týchto notifikovaných osôb s požiadavkami stanovenými v príslušných ustanoveniach Nariadenia (čl.33 Nariadenia).
Orgán posudzovania zhody	Orgán, ktorý ako tretia strana vykonáva činnosti posudzovania zhody vrátane skúšania,	kompetencie notifikovanej osoby po splnení notifikačného procesu predpokladaného Nariadením;	Viď poznámky k notifikovaným osobám vyššie.

Inštitúcia	Základná definícia	Základné kompetencie	Poznámka ³⁸
(čl. 3 ods. 1 bod 21 Nariadenia)	certifikácie a kontroly v zmysle Nariadenia. Posudzovanie zhody je postup preukazovania, či boli splnené požiadavky stanovené v hlave III kapitole 2 Nariadenia týkajúce sa vysokorizikového systému umelej inteligencie.	• <u>zohľadňovanie správ o výstupoch z AI sandboxu vypracovaných zriaďujúcim orgánom v kontexte postupov posudzovania zhody.</u>	
Európsky úrad pre umelú inteligenciu (Úrad) (čl. 56 ods. 1 Nariadenia)	Nezávislý orgán EÚ s vlastnou právnou subjektivitou s kompetenciami v oblasti Nariadenia.	• prispieva k účinnej spolupráci vnútroštátnych dozorných orgánov a Komisie, pokiaľ ide o záležitosti, na ktoré sa vzťahuje Nariadenie; • koordinuje a prispieva k usmerneniam a analýze, ktoré poskytujú Komisia a vnútroštátne dozorné orgány, ako aj ďalšie príslušné orgány k problémom vznikajúcim na vnútornom trhu v súvislosti so záležitosťami, na ktoré sa vzťahuje Nariadenie; • pomáha vnútroštátnym dozorným orgánom a Komisii pri zabezpečovaní konzistentného uplatňovania Nariadenia	Zriaďujúci orgán informuje Úrad o zriadení AI sandboxu a môže požiadať o podporu a usmernenie.

2.1.2. Základný okruh OVM SR a ostatných zainteresovaných osôb vo vzťahu k zriadeniu sandboxu pre umelú inteligenciu predpokladaného Nariadením v podmienkach SR

V súvislosti s definovaním OVM SR potenciálne dotknutých požiadavkami Nariadenia vo vzťahu k zriaďovaniu a fungovaniu sandboxov pre umelú inteligenciu v zmysle Nariadenia uvádzame v Tabuľke č. 2 základný prehľad OVM SR, iných relevantných orgánov/inštitúcií a ďalších relevantných subjektov, ktoré boli v tejto súvislosti identifikované. Identifikácia OVM, ktoré by mohli byť určené ako vnútroštátne dozorné orgány a/alebo orgány zriaďujúce sandbox pre umelú inteligenciu v zmysle Nariadenia, je len orientačná, pričom členské štáty majú v tejto oblasti značnú voľnosť a bude predmetom ďalšieho hodnotenia na strane relevantných OVM SR okrem iného s prihliadnutím na závery a odporúčania TSI Analýzy.

Tabuľka č.2 Prehľad relevantných OVM SR a ostatných zainteresovaných osôb vo vzťahu k zriadeniu sandboxu predpokladaného Nariadením v podmienkach SR

Orgán	Kompetencie	Potenciálny vzťah k zriadeniu a fungovaniu AI sandboxu
Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (MIRRI)	OVM s delegovanou zodpovednosťou za koordináciu Akčného plánu digitálnej transformácie Slovenska na roky 2023 – 2026 (ďalej len „APDTS“) a naň nadväzujúce programy a ústredný orgán štátnej správy pre oblasť centrálného riadenia informatizácie spoločnosti a tvorbu politiky jednotného digitálneho trhu.	Gestor zriadenia experimentálnych regulačných prostredí pre AI na základe Opatrenia 3.1.1.7 Akčného plánu digitálnej transformácie Slovenska na roky 2023 – 2026. V nadväznosti na ďalšie hodnotenie (napr. aj s prihliadnutím na výsledky TSI Analýzy v relevantnom rozsahu), môže byť MIRRI jedným z orgánov, ktoré môžu byť určené ako vnútroštátny dozorný orgán a/alebo orgán zriaďujúci AI sandbox v zmysle Nariadenia.
Rada vlády Slovenskej republiky pre digitalizáciu verejnej správy a jednotný digitálny trh	Poradný, koordinačný a iniciatívny orgán vlády Slovenskej republiky (ďalej len „vláda“) pre otázky týkajúce sa informatizácie, jednotného digitálneho trhu a digitalizácie verejnej správy orientovanej na poskytovanie elektronických služieb verejnej správy pre právnické osoby a fyzické osoby, ako aj rozvoja ekonomického prostredia na Slovensku smerom k digitálnej ekonomike.	Zapojenie do koordinácie procesov a legislatívnych iniciatív súvisiacich s implementáciou požiadaviek Nariadenia, vrátane definície inštitucionálneho rámca predpokladaného Nariadením a alokácie zodpovednosti za zriadenie a fungovanie AI sandboxu.
Legislatívna rada vlády Slovenskej republiky	Stály poradný a koordinačný orgán vlády v oblasti legislatívy.	Koordinácia legislatívnych iniciatív súvisiacich s implementáciou požiadaviek Nariadenia, vrátane definície inštitucionálneho rámca predpokladaného Nariadením a alokácie zodpovednosti za zriadenie a fungovanie AI sandboxu.
Stála komisia pre etiku a reguláciu umelej inteligencie (CERAI)	Nezávislý odborný a poradný orgán zriadený MIRRI pre oblasť posudzovania etických, sociálno-spoločenských a právnych otázok súvisiacich s výskumom, vývojom, nasadzovaním a používaním technológií využívajúcich prvky a systémy AI.	Potenciálne zapojenie do procesu zriadenia a fungovania sandboxu pre umelú inteligenciu (napr. nastavenie pravidiel fungovania AI sandboxu, hodnotenie projektov, <i>ad hoc</i> konzultácie) ⁴¹ v kontexte povinnosti (najmä zriaďujúceho orgánu) uľahčiť zapojenie ďalších relevantných aktérov v rámci ekosystému umelej inteligencie s cieľom

⁴¹ Viď najmä časť 4.3.2 Štúdie.

Orgán	Kompetencie	Potenciálny vzťah k zriadeniu a fungovaniu AI sandboxu
		umožniť a uľahčiť spoluprácu s verejným a súkromným sektorom pri prevádzke sandboxu (viď čl. 53a bod 2 písm. d) Nariadenia).
Úrad na ochranu osobných údajov Slovenskej republiky (ÚOOÚ)	Orgán štátnej správy, ktorý vykonáva dozor nad ochranou osobných údajov.	Zapojenie/spolupráca pri (i) prevádzke sandboxu, pokiaľ inovačné systémy umelej inteligencie spracúvajú osobné údaje, a (ii) dohľade nad jeho aspektmi v príslušnom rozsahu (viď. napr. čl. 53 ods. 2 Nariadenia). V nadväznosti na ďalšie hodnotenie (napr. aj s prihliadnutím na výsledky TSI Analýzy v relevantnom rozsahu), môže byť ÚOOÚ jedným z orgánov, ktoré môžu byť určené ako vnútroštátny dozorný orgán a/alebo orgán zriaďujúci AI sandbox v zmysle Nariadenia.
Slovenská národná akreditačná služba (SNAS)	Verejnoprávna inštitúcia poskytujúca akreditačné služby v zmysle Zákona o akreditácii ⁴² .	SNAS môže byť určená ako „notifikujúca osoba“ v zmysle Nariadenia notifikujúca orgány posudzovania zhody, ktoré v zmysle Nariadenia majú zohľadňovať správy o výstupoch vypracované zriaďujúcim orgánom sandboxu pre umelú inteligenciu v kontexte postupov posudzovania zhody. Možné zapojenie do procesu zriaďovania a fungovania AI sandboxu vo vzťahu k definovaniu vzťahov s príslušnými procesmi a orgánmi posudzovania zhody alebo iných aspektov (viď nižšie).
Ministerstvo hospodárstva Slovenskej republiky / ostatné orgány dohľadu nad trhom (napr. SOI, ŠÚKL – viď časť 2.1.1 Štúdie vyššie) / iní sektoroví regulátori (vo vzťahu k NBS/ÚRSO viď tiež riadok nižšie)	Jednotný úrad pre spoluprácu v zmysle čl. 10 ods. 3 Nariadenia 2019/1020 / orgány dohľadu (nad trhom) v zmysle príslušných sektorových predpisov	Orgány dohľadu nad trhom majú zohľadňovať správy o výstupoch vypracované zriaďujúcim orgánom sandboxu pre umelú inteligenciu v kontexte kontrol v rámci dohľadu nad trhom. Zapojenie do procesu zriaďovania a fungovania AI sandboxu vo vzťahu k definovaniu vzťahov s príslušnými procesmi a orgánmi dohľadu nad trhom. Spolupráca so zriaďujúcim orgánom vo veciach dohľadu týkajúcich sa prevádzkovania AI sandboxu v rozsahu svojich úloh a právomocí (viď najmä čl. 53 ods. 2 Nariadenia). Spolupráca pri podpore poskytovania vysokokvalitných údajov na tréning, validáciu a testovanie systémov umelej inteligencie v rámci AI sandboxu (viď napr. odôvodnenie (45) Nariadenia). Ďalšie možnosti zapojenia v rozsahu napr. (i) konzultácií pri definovaní základných parametrov AI sandboxu (napr. kritériá pre vstup, hodnotenie), (ii) participácia na prevádzke AI sandboxu (zapojenie zástupcov orgánov do hodnotiacich/kontrolných komisií/orgánov) ⁴³ , a (iii) hodnotenia

⁴² Zákon č. 53/2023 Z. z. o akreditácii orgánov posudzovania zhody (ďalej len „Zákon o akreditácii“).

⁴³ Viď najmä časť 4.3.2 Štúdie.

Orgán	Kompetencie	Potenciálny vzťah k zriadeniu a fungovaniu AI sandboxu
		funkčnosti AI sandboxu a definovania podnetov na zefektívnenie jeho fungovania.
Národná banka Slovenska (NBS)	Nezávislá centrálna banka Slovenskej republiky s pôsobnosťou v oblasti dohľadu nad finančným trhom SR. NBS má byť orgánom dohľadu nad trhom v prípade systémov umelej inteligencie, ktoré uvádzajú na trh, do prevádzky alebo používajú finančné inštitúcie regulované právnymi predpismi EÚ o finančných službách.	Vid' vysvetlenia v riadku vyššie. Možné zapojenie do procesu zriaďovania AI sandboxu zdieľaním skúseností a tzv. best practices získaných v súvislosti s prevádzkovaním regulačného sandboxu NBS (vid' časť 3.1.3.4 Štúdie nižšie) (to isté platí aj vo vzťahu k ÚRSO, ktorý je sektorovým regulátorom pre oblasť sieťových odvetví a prevádzkuje sandbox ÚRSO).
Národný bezpečnostný úrad (NBÚ)	Ústredný orgán štátnej správy na ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby.	OVM, ktorý môže byť zapojený do procesu zriaďovania a fungovania AI sandboxu vo viacerých rovinách (vid' vyššie), ako aj v rámci (i) spolupráce pri definovaní štandardov kybernetickej bezpečnosti pre fungovanie AI sandboxu (vrátane jeho technologického riešenia – vid' časť 5 Štúdie, (ii) (spolu)účasti na príprave usmernení pre účastníkov AI sandboxu dotýkajúcich sa oblasti kybernetickej bezpečnosti, a (iii) prevádzke sandboxu (napr. zapojenie zástupcov do hodnotiacich/kontrolných komisií/orgánov). V nadväznosti na ďalšie hodnotenie (napr. aj s prihliadnutím na výsledky TSI Analýzy v relevantnom rozsahu), môže byť NBÚ jedným z orgánov, ktoré môžu byť určené ako vnútroštátny dozorný orgán a/alebo orgán zriaďujúci sandbox v zmysle Nariadenia.
Relevantní aktéri v rámci ekosystému umelej inteligencie (v zmysle čl. 53a bodu 2 písm. d) Nariadenia) - notifikované osoby (vid' časť 2.1.1 vyššie) a normalizačné organizácie, MSP, startupy, podniky, inovátori, testovacie a experimentálne zariadenia, výskumné a experimentálne laboratória a centrá digitálnych inovácií, centrá excelentnosti (vid' tiež nižšie), jednotliví výskumní pracovníci ⁴⁴	V zmysle čl. 53a bodu 2 písm. d) Nariadenia je potrebné, aby nastavenie sandboxov uľahčovalo zapojenie ďalších relevantných aktérov s cieľom umožniť a uľahčiť spoluprácu s verejným a súkromným sektorom.	Široký rozsah možností zapojenia relevantných aktérov do procesu zriaďovania a fungovania sandboxu, vrátane (i) konzultácií pri definovaní základných parametrov sandboxu (napr. kritériá pre vstup, hodnotenie), (ii) participácia na prevádzke sandboxu (zapojenie zástupcov do hodnotiacich/kontrolných komisií/orgánov), a (iii) hodnotenia funkčnosti sandboxu a definovania podnetov na zefektívnenie jeho fungovania.

⁴⁴ Ako príklad možno uviesť napr. Slovenské centrum pre výskum umelej inteligencie – slovak.AI, Národné kompetenčné centrum pre vysokovýkonné počítače a pod.

2.2 Zodpovednosti aktérov realizácie sandboxu pre umelú inteligenciu predpokladaného Nariadením

V predchádzajúcej časti 2.1.2. Štúdie bol predstavený základný prehľad relevantných OVM SR a ostatných zainteresovaných osôb, ktoré prichádzajú do úvahy v súvislosti so zriadením a následnou realizáciou experimentálneho regulačného prostredia pre umelú inteligenciu - AI sandboxu tak, ako ho predpokladá Nariadenie. Nižšie budeme z tohto prehľadu vychádzať, pričom sa zameriame na konkrétne zodpovednosti typických aktérov, ktorí sú v praxi priamo a bezprostredne zapojení do samotného procesu prevádzky AI sandboxu a posudzovania testovaného AI systému v sandboxe. Pre potreby identifikácie týchto zodpovedností sme jednotlivých aktérov zoskupili do hlavných rolí, v rámci ktorých sa budú zapájať do uvedeného procesu. Hlavné role boli identifikované nasledovne:

- 1) **Regulačný orgán:** V kontexte Nariadenia najmä OVM zriaďujúci AI sandbox s primárnou zodpovednosťou za zriadenie a fungovanie AI sandboxu.
- 2) **Účastníci sandboxu pre umelú inteligenciu:** Organizácie alebo subjekty, ktoré prihlasujú svoje AI systémy/riešenia do AI sandboxu a testujú ich v rámci prevádzky AI sandboxu.
- 3) **Koncoví používatelia:** Osoby alebo skupiny, ktoré môžu byť ovplyvnené AI systémami testovanými v sandboxe, a ktorých názory a skúsenosti sú dôležité pre hodnotenie účinnosti a bezpečnosti.
- 4) **Ostatné zúčastnené orgány dohľadu:** Ostatné regulačné orgány/orgány dohľadu (vrátane orgánov dohľadu nad trhom), ktoré môžu byť zapojené a/alebo spolupracovať na prevádzke AI sandboxu alebo pri dohľade nad jednotlivými aspektmi v sandboxe testovaných systémov.
- 5) **Ďalší relevantní aktéri v rámci ekosystému umelej inteligencie** (v zmysle čl. 53a bodu 2 písm. d) Nariadenia) - notifikované osoby (viď časť 2.1.1. vyššie) a normalizačné organizácie, MSP, startupy, podniky, inovátori, testovacie a experimentálne zariadenia, výskumné a experimentálne laboratória a centrá digitálnych inovácií, centrá excelentnosti, vrátane zástupcov občianskej spoločnosti a ďalšie relevantné subjekty - ďalší aktéri, ktorí sa môžu v rôznych formách podieľať na procese zriaďovania a fungovania AI sandboxu a participovať na rozvoji AI ekosystému na Slovensku.

Tabuľka č.3. Prehľad typických zodpovedností aktérov sandboxov pre umelú inteligenciu

Rola	Zodpovednosti
Regulačný orgán zriaďujúci sandbox (v kontexte Nariadenia - zriaďujúci orgán)	- Dozoruje a monitoruje testovanie nových systémov AI v sandboxe, aby zabezpečil súlad s platnými predpismi (v kontexte tejto Štúdie pôjde najmä o Nariadenie) a právnymi normami týkajúcimi sa ochrany údajov, etiky, bezpečnosti a ďalších relevantných oblastí. - Poskytuje podporu a usmernenie pre subjekty zapojené do sandboxu pri aplikácii právnych predpisov a zároveň sa snaží minimalizovať riziká a potenciálne negatívne dôsledky nových AI technológií. - Zhromažďuje a analyzuje informácie z testovania AI v sandboxe, aby lepšie porozumel súvislostiam a účinkom nových technológií v konkrétnych oblastiach, čo mu pomáha prispieť k tvorbe alebo revízii príslušných právnych predpisov. - Komunikuje s účastníkmi AI sandboxu a ďalšími zainteresovanými stranami, aby získal spätnú väzbu, pochopil ich potreby a obavy a zabezpečil lepšie

Rola	Zodpovednosti
	vytváranie a uplatňovanie pravidiel pre AI v rámci právneho systému a regulácie vo všeobecnosti. • Spolupracuje s ďalšími orgánmi na národnej alebo medzinárodnej úrovni, v kontexte Nariadenia najmä orgánmi dohľadu nad trhom a orgánmi posudzovania zhody (notifikovanými osobami), aby zabezpečil metodiku a dohľad vo vzťahu k AI systémom testovaným v rámci sandboxu v rozsahu ich právomocí, zdieľal poznatky, osvedčené postupy a spoločne pracoval na vytváraní efektívnych prístupov k regulácii AI.
Účastník sandboxu	• Účastník musí dodržiavať všetky pravidlá a predpisy stanovené právnymi normami a dohodnuté s regulačným orgánom počas svojej účasti v AI sandboxe. • Účastník by mal pravidelne informovať regulačný orgán o pokroku, výsledkoch a všetkých zistených rizikách pri testovaní svojej AI technológie. • Účastník musí mať na zreteli všeobecnú bezpečnosť a ochranu údajov v rámci všetkých testov a aktivít v sandboxe. Musí prijať opatrenia na minimalizáciu rizika úniku údajov alebo iných bezpečnostných hrozieb. • Účastník by mal úzko spolupracovať so všetkými zúčastnenými orgánmi spolupracujúcimi pri prevádzke AI sandboxu a byť ochotný poskytnúť potrebné informácie, keď je to požadované. • Účastník by mal aktívne identifikovať a riadiť všetky riziká spojené s používaním jeho AI systémov a byť pripravený implementovať opatrenia na ich minimalizáciu v spolupráci s príslušnými OVM a najmä zriaďujúcim orgánom. • Účastník by mal udržiavať detailnú dokumentáciu všetkých testov, výsledkov a zmien vykonaných v rámci sandboxu v zmysle požiadaviek a byť transparentný voči príslušným orgánom a ďalším zainteresovaným stranám.
Koncový používateľ technológie	• Poskytovanie relevantnej a užitočnej spätnej väzby týkajúcej sa funkčnosti, účinnosti a bezpečnosti AI systému počas testovania. • Rešpektovanie pravidiel a noriem stanovených regulačným rámcom pre testovanie AI technológií a dodržiavanie určených postupov a obmedzení. • Aktívna identifikácia možných problémov, chýb alebo rizík, ktoré môžu vzniknúť pri používaní AI systémov (vrátane testovania v reálnych podmienkach) a ich oznamovanie orgánom dohľadu (napr. v zmysle Nariadenia vnútroštátnemu dozornému orgánu a/alebo iným orgánom dohľadu nad trhom). • Spolupráca s príslušnými orgánmi v rámci možností stanovených právnym rámcom, vrátane účasti na potrebných posudkoch a hodnoteniach AI systémov, aby sa zabezpečilo dodržiavanie noriem a predpisov. • Informovanosť o zmenách a aktualizáciách v predpisoch týkajúcich sa AI systémov a získavanie informácií o ich správnom používaní.
Ostatné zúčastnené orgány dohľadu (v kontexte Nariadenia najmä orgány dohľadu nad trhom)	• Poskytovanie odborných znalostí a poradenstva týkajúce sa systémov umelej inteligencie a ich aplikácie v rámci ich sektorovej kompetencie, v spolupráci s orgánom zriaďujúcim AI sandbox, pre účely metodických usmernení ohľadom technických a praktických aspektov projektov v sandboxe a zabezpečenie dohľadu. • Pomáhanie pri identifikácii a hodnotení rizík spojených s AI systémami, aby sa minimalizovali možné negatívne dôsledky a chránili zúčastnené strany. • Poskytovanie metodickej podpory a pomoci pri implementácii AI systémov tak, aby boli v súlade s príslušnými predpismi a štandardmi. • Aktívna spolupráca s regulačnými orgánmi na zabezpečenie dodržiavania pravidiel a smerníc v rámci AI sandboxu.

Rola	Zodpovednosti
	• Zdieľanie poznatkov, skúseností a najlepších postupov so zainteresovanými stranami a orgánmi (vrátane zriaďujúceho orgánu) na podporu zlepšenia regulácie a využitia AI technológie v praxi.
Ďalší relevantní aktéri	• Ako už bolo uvedené vyššie, táto skupina zahŕňa širokú skupinu subjektov, pričom vo vzťahu k týmto aktérom existuje široký okruh možností ich zapojenia do procesu zriaďovania a fungovania AI sandboxu, vrátane (i) konzultácií pri definovaní základných parametrov sandboxu (napr. kritériá pre vstup, hodnotenie), (ii) participácia na prevádzke AI sandboxu (zapojenie zástupcov do hodnotiacich/kontrolných komisií/orgánov), a (iii) hodnotenia funkčnosti AI sandboxu a definovania podnetov na zefektívnenie jeho fungovania. • V prípade zástupcov občianskej spoločnosti ako jednej z kategórií relevantných aktérov ich úlohou je typicky zastupovať záujmy a potreby verejnosti v súvislosti s vývojom a využívaním AI systémov, vrátane zberu a komunikácie názorov, obáv a pripomienok od občanov a ich zdieľanie prostredníctvom príslušných komunikačných kanálov, vrátane kanálov potenciálne zriadených v rámci regulačného sandboxu. • V širšom kontexte sa títo aktéri podieľajú na verejnej kontrole pôsobenia sandboxu a prispievajú do diskusie o etickom a zákonnom využívaní AI systémov. Ak sú identifikované nedostatky, mali by na nich poukazovať a zdôrazňovať ich dôležitosť. • Zodpovedajú za osvetu a šírenie informácií o regulácii AI v rámci ich možností a kompetencií a poskytovanie vzdelávacích materiálov verejnosti okrem iného s cieľom zabezpečiť, aby ľudia rozumeli dopadom AI a mali možnosť sa zapojiť do diskusií.

2.3 Analýza dopadov zavedenia experimentálneho regulačného prostredia (sandboxu) na dotknuté zainteresované osoby

Vytvorenie sandboxu pre umelú inteligenciu by malo viaceré kľúčové dopady na Slovensko a jeho technologický sektor. Zavedenie takéhoto experimentálneho regulačného prostredia by mohlo viesť k zvýšenej inovácii a rozvoju technológií umelej inteligencie v krajine a zároveň k podpore vzniku nových spoločností v sektore, ktoré by mohli vytvárať nové pracovné miesta a prilákať ďalšie investície na Slovensko. Avšak s touto iniciatívou prichádzajú aj potenciálne riziká a dôsledky, ktoré treba analyzovať a prijatými opatreniami minimalizovať ich negatívny dopad.

Nedostatok prísnych noriem a dohľadu by mohol viesť k situáciám, kde by boli občianske slobody a súkromie ohrozené v dôsledku neoprávneného zhromažďovania dát alebo neetického použitia umelej inteligencie. Ďalším dôležitým aspektom je riziko vytvorenia technológií AI, ktoré by mohli vytvárať nerovnováhu alebo diskriminovať určitú skupinu obyvateľstva. Bez dostatočnej regulácie by sa mohlo stať, že tieto technológie by mohli byť zamerané iba na určitú časť spoločnosti alebo zvýrazňovať existujúce nerovnosti.

Všeobecné dopady zavedenia AI sandboxu na prostredie slovenského technologického sektora sú v nasledujúcej tabuľke rozdelené na možné pozitívne dopady, negatívne dopady, príležitosti a hrozby.

Tabuľka č.4. Všeobecné dopady, príležitosti a hrozby zavedenia sandboxu pre umelú inteligenciu na prostredie slovenského technologického sektora

Pozitívne dopady	Negatívne dopady
Inovácie a vývoj: Sandbox môže podporiť inovácie a technologický rozvoj v oblasti umelej inteligencie prostredníctvom testovania nových nápadov a produktov. Flexibilita a pružnosť: Možnosť experimentovania s novými AI technológiami umožní prispôsobenie a aktualizáciu existujúcich regulácií podľa aktuálnych potrieb a trendov. Podpora konkurencie: Sandbox môže stimulovať konkurenciu medzi spoločnosťami, čo môže viesť k lepším službám a produktom pre spotrebiteľov.	Nedostatočná regulácia: Nedostatok jasných noriem a pravidiel môže viesť k nejednoznačnosti a riziku zneužívania AI technológií. Finančné náklady: Implementácia a správa regulačného sandboxu môže byť nákladná, čo môže obmedziť jeho dostupnosť a účinnosť. Bezpečnostné riziká: Testovanie nových technológií môže predstavovať bezpečnostné riziká, ak nie sú stanovené dostatočné opatrenia na ochranu údajov a súkromia.
Príležitosti	Hrozby
Podpora inovácií: Sandbox môže vytvoriť prostredie, ktoré povedie k vývoju nových AI aplikácií s vysokou pridanou hodnotou. Zlepšenie právnych predpisov: Skúsenosti zo sandboxu môžu poskytnúť dôležité informácie na zlepšenie existujúcich právnych predpisov týkajúcich sa umelej inteligencie. Medzinárodná konkurencieschopnosť: Vytvorenie priaznivého prostredia pre AI inovácie môže posilniť medzinárodnú pozíciu Slovenska v technologickom sektore.	Etické obavy: Nedostatočné sledovanie etických aspektov AI v sandboxe môže viesť k spoločenskému nesúhlasu a strate dôvery verejnosti. Riziko neúspechu testovania: Možnosť zlyhania nových technológií v raných fázach testovania môže viesť k negatívnym dôsledkom a znevýhodneniu účastníkov sandboxu. Odpoveď regulačných orgánov: Neistota alebo pomalá reakcia regulačných orgánov na nové technologické výzvy môže mať za následok nedostatočnú ochranu spotrebiteľov a ich práv.

2.3.2 Podnikateľské subjekty

Pri zavádzaní sandboxu pre umelú inteligenciu do podnikateľského prostredia sa očakávajú rôzne dôsledky, ktoré môžu ovplyvniť podniky a ich inovácie. Tento prístup otvára nové možnosti, ale súčasne prináša aj určité riziká.

Tabuľka č.5 Dopady zavedenia sandboxu pre umelú inteligenciu v prostredí SR na podnikateľské subjekty

Pozitívne dopady	Negatívne dopady
Podpora inovácií: Sandbox môže podporiť inovácie v oblasti AI, pretože umožňuje podnikom testovať nové technológie a riešenia pod regulačným dohľadom. To môže viesť k vytvoreniu nových produktov a služieb. Zrýchlenie vývoja: Možnosť experimentovať v rámci sandboxu umožňuje rýchlejší vývoj AI aplikácií a technológií. Tento pružný rámec môže pomôcť podnikom prispôbiť sa rýchlo meniacemu sa prostrediu a zlepšiť konkurencieschopnosť. Spolupráca s regulačnými orgánmi: Zavedenie sandboxu môže viesť k lepšej spolupráci medzi podnikmi a regulačnými orgánmi. Táto spolupráca môže umožniť vytvorenie vhodnejších pravidiel a smerníc pre umelú inteligenciu na trhu.	Riziko zneužitia: Nedostatočná regulácia v sandboxe môže viesť k zneužitiu AI technológií. Podniky by mohli využiť tento testovací rámec prípadne určité úľavy z regulačných povinností na implementáciu rizikových alebo škodlivých aplikácií, čo by mohlo mať nepriaznivý vplyv na spoločnosť a spotrebiteľov. Nadmerné riziko a neistota: Pre niektoré podniky môže byť sandbox spojený s nadmerným rizikom a neistotou. Absencia jasnej regulácie a určených postupov môže spôsobiť obavy a odstrašiť niektoré subjekty od účasti. Nedostatok zdrojov: Niektoré podnikateľské subjekty môžu mať obmedzené finančné a ľudské zdroje na to, aby využili výhody sandboxu. To môže viesť k nerovnomernému prístupu a obmedzenej účasti.

2.3.3 Orgány verejnej moci - Regulačné orgány

Súčasný trend rozvoja umelej inteligencie prináša so sebou nové výzvy a príležitosti pre orgány verejnej moci (OVM) a ich reguláciu, vrátane príslušných OVM v Slovenskej republike. Zavedenie sandboxu pre AI môže byť dôležitým krokom, ktorý má potenciál prispieť k inováciám, ale zároveň so sebou prináša niektoré neistoty a riziká.

Tabuľka č.6 Dopady zavedenia sandboxu na orgány verejnej moci SR

Pozitívne dopady	Negatívne dopady
Podpora inovácií a vývoja: Spustenie sandboxu vytvára vhodné prostredie pre testovanie nových AI projektov bez prílišnej byrokracie a obmedzení. To môže povzbudiť inovácie a podporiť vývoj technológií, čo môže prispieť k ekonomickej konkurencieschopnosti krajiny. Flexibilita v regulácii: Tento prístup umožňuje pružnosť pri stanovovaní noriem a predpisov pre umelú inteligenciu. OVM môžu získať cenné poznatky a skúsenosti, ktoré im pomôžu prispôbiť reguláciu tak, aby bola účinnejšia a primeranejšia pre rýchlo sa meniace technologické prostredie. Podpora pre malé a stredné podniky: Vytvorenie sandboxu pre umelú inteligenciu umožní menším a stredným podnikom s obmedzenými zdrojmi testovať svoje inovatívne riešenia bez veľkých nákladov na dodržiavanie prísnych predpisov, čo predstavuje jeden zo základných cieľov a jednu z prioritných požiadaviek definovaných Nariadením.	Riziko zneužitia: Nedostatok prísnych noriem a kontroly môže viesť k možnému zneužitiu technológií na úkor ochrany údajov, súkromia a etiky. Regulačné orgány sa budú musieť pripraviť na predchádzanie takémuto zneužitiu prostredníctvom včasnej implementácie efektívnej regulácie. Nedostatok jednotnej regulácie: Prítomnosť sandboxu by mohla spôsobiť fragmentáciu regulácie, v rámci ktorej by rôzne regióny alebo sektory mali odlišné pravidlá a normy pre umelú inteligenciu. Toto môže spôsobiť zmatečné prostredie pre podniky a spotrebiteľov a tým brániť efektívnemu využitiu technológií. Ťažkosti s monitorovaním a vynucovaním: Pôsobenie v sandboxe môže byť obtiažne monitorované a vynucované z hľadiska dodržiavania noriem, keďže toto prostredie je určené pre experimentovanie a nové nápady. Toto môže vytvoriť výzvy pre OVM pri zabezpečovaní bezpečnosti a zhody s právnymi predpismi.

2.3.4 Zákazníci - koncoví používatelia

Zavedenie sandboxu pre umelú inteligenciu prinesie so sebou rôzne dôsledky aj pre zákazníkov a koncových používateľov. Tieto dôsledky môžu byť pozitívne aj negatívne a budú mať vplyv na ich skúsenosti s technológiou AI.

Tabuľka č.7. Dopady zavedenia regulačného sandboxu na koncových používateľov

Pozitívne dopady	Negatívne dopady
Inovácie a lepšie služby: Zriadenie regulačného sandboxu umožňuje podnikom experimentovať s AI a inováciami so zníženým rizikom neplnenia existujúcich noriem. To môže viesť k vývoju nových produktov a služieb, ktoré sú lepšie prispôbené potrebám zákazníkov. Zvyšovanie dôvery a transparentnosti: Regulačný sandbox môže posilniť dôveru zákazníkov voči technológiám AI tým, že prinesie transparentnosť a jasnosť v procese vývoja a implementácie nových riešení. Táto transparentnosť môže zvýšiť povedomie zákazníkov o tom, ako AI systémy fungujú a aké sú ich obmedzenia.	Bezpečnostné a etické riziká: Sandboxy môžu vytvoriť priestor pre vznik bezpečnostných a etických rizík. Experimenty s AI bez prísnych regulácií môžu viesť k vytváraniu systémov, ktoré nie sú dostatočne chránené pred zneužitím alebo nežiadúcimi dôsledkami, čo môže ohroziť bezpečnosť a súkromie koncových používateľov. Nerovnováha vo vzťahu medzi firmami a používateľmi: Príliš veľká voľnosť pre podniky v rámci sandboxu môže viesť k nerovnováhe vo vzťahu medzi firmami a koncovými používateľmi. Ak sa podniky sústredia len na svoje vlastné ciele a minimalizujú ochranu a záujmy používateľov, môže to viesť k vykorisťovaniu a zneužívaniu ich údajov a dôvery.

2.3.5 Ďalší relevantní aktéri v rámci ekosystému umelej inteligencie

Vytvorenie sandboxu pre umelú inteligenciu môže mať dopady aj pre ďalších aktérov v rámci ekosystému umelej inteligencie v Slovenskej republike. V tomto kontexte rozumieme ďalších aktérov tak, ako sú definovaní v časti 2.1.2 Štúdie vyššie. Je nevyhnutné starostlivo zvažovať výhody a nevýhody tejto iniciatívy a prispôbiť ju tak, aby podporovala rozvoj a inovácie v oblasti umelej inteligencie s ohľadom na etické, právne a finančné aspekty.

Tabuľka č.8. Dopady zavedenia regulačného sandboxu na akademickú obec

Pozitívne dopady	Negatívne dopady
Inovácie a Výskum: Spustenie sandboxu pre umelú inteligenciu by umožnilo akademickým subjektom testovať nové AI aplikácie, algoritmy a technológie v kontrolovanom prostredí. To by mohlo povzbudiť študentov a výskumníkov k vytváraniu nových a lepších prístupov k AI, čo by v konečnom dôsledku prispelo k rozvoju nových poznatkov a technologických riešení. Spolupráca s priemyslom: Sandbox by mohol vytvoriť príležitosť na väčšiu spoluprácu medzi akademickými subjektmi a priemyslom. Tento proces by umožnil výskumníkom a študentom pracovať na reálnych projektoch v spolupráci so súkromnými firmami. Vzdelávanie a odbornosť: Sandbox by mohol poskytnúť akademickým subjektom príležitosť posilniť vzdelávanie týkajúce sa etických, právnych a bezpečnostných aspektov AI. Tým by sa vytvoril priestor pre odbornú prípravu študentov a výskumníkov v oblastiach, ktoré sú kritické pre zodpovedné a bezpečné využívanie systémov umelej inteligencie. Participácia na hodnotení: Výskumníci a odborníci z univerzít a výskumných centier môžu poskytnúť odborné poznatky a analytickú podporu na vyhodnotenie rizík a prínosov AI v regulovanom prostredí.	Etické a právne otázky: Testovanie nových aplikácií a algoritmov by mohlo vyvolať situácie, kde sa konfrontujú etické dilemy alebo porušujú právne predpisy. To môže viesť k neistote a potrebe prísnejšieho dohľadu nad týmito aktivitami. Finančné a zdrojové nároky: Pre akademické subjekty, ktoré môžu mať obmedzený rozpočet, môže táto iniciatíva znamenať ťažkosti v zabezpečovaní potrebných zdrojov na participáciu a aktívne zapojenie sa do sandboxu pre umelú inteligenciu. Závislosť od regulačných opatrení: Existuje riziko, že akademické subjekty sa môžu stať príliš závislými od regulačných opatrení v rámci sandboxu pre umelú inteligenciu. To by mohlo obmedziť ich schopnosť experimentovať a inovovať mimo tohto regulačného rámca, čo by mohlo brzdiť ich potenciálny pokrok v AI výskume.

3 Analýza súčasného stavu implementácie riešení umelej inteligencie (AI) a právneho rámca pre zriadenie sandboxov v zmysle Nariadenia a slovenskej legislatívy

Nasledujúce časti Štúdie obsahujú zhrnutie aktuálneho stavu legislatívy v oblasti regulácie umelej inteligencie na Slovensku (časť 3.1 nižšie), a analýzu legislatívneho rámca pre implementáciu sandboxov pre umelú inteligenciu (časť 3.1.1 nižšie) tak v zmysle právneho rámca predpokladaného Nariadením (vrátane špecifických požiadaviek na ich fungovanie) časť 3.1.2 nižšie) a aktuálneho legislatívneho prostredia SR (časť 3.1.3 nižšie). V tejto súvislosti zároveň zhrnieme legislatívno-technické možnosti zavedenia sandboxu v Slovenskej republike, vrátane odporúčaní pre zriadenie sandboxu pre umelú inteligenciu v prostredí Slovenskej republiky (viď najmä časť 3.3 nižšie).

3.1 Analýza súčasného stavu právneho rámca implementácie AI riešení na Slovensku

V podmienkach Slovenskej republiky v súčasnosti neexistuje osobitná komplexná legislatívna úprava pre umelú inteligenciu, pričom táto oblasť bude komplexne regulovaná Nariadením a s ním súvisiacimi delegovanými a implementačnými predpismi. V tejto oblasti teda nie sú zatiaľ prijaté žiadne právne predpisy, ktoré by problematiku umelej inteligencie komplexne upravovali s výnimkou parciálnej regulácie v špecifických oblastiach.⁴⁵

V dôsledku toho sa využívanie a rozvoj systémov AI na Slovensku aktuálne riadi primárne všeobecným právnym rámcem a všeobecnými princípmi aplikácie práva, a to najmä v nasledovných oblastiach:

- **ochrana osobných údajov** - pokiaľ systém umelej inteligencie spracováva osobné údaje, musí sa toto spracúvanie vykonávať v súlade s predpismi o ochrane osobných údajov, a to najmä zákonom č. 18/2018 Z.z. o ochrane osobných údajov v znení neskorších predpisov ako aj GDPR;
- **zodpovednosť za škodu** - režim zodpovednosti za škodu má okrem iného priamu súvislosť aj s otázkami právnej subjektivity umelej inteligencie. Keďže v súčasnosti je z právneho hľadiska umelá inteligencia vecou, ktorá je objektom právneho vzťahu, zodpovednosť za spôsobenú škodu vychádza z konceptu prechodu na prevádzkovateľa resp. vlastníka veci.⁴⁶ V tejto súvislosti tiež možno uviesť, že v súčasnosti by režim zodpovednosti za použitie systému umelej inteligencie zrejme vychádzal z konceptu všeobecnej zodpovednosti za škodu najmä podľa ust. §420 a nasl. Občianskeho zákonníka⁴⁷, prípadne Zákona o zodpovednosti za škodu spôsobenú vadným výrobkom⁴⁸ (ak je jeho komponentom systém umelej inteligencie) a ďalších súvisiacich predpisov (vrátane predpisov EÚ). Po implementácii Smernice o zodpovednosti do právneho poriadku SR sa bude zodpovednostný režim riadiť modifikáciami zavádzanými Smernicou o zodpovednosti (viď aj časť 1.2.1 vyššie);

⁴⁵ Viď napr. Odborné usmernenie Ministerstva zdravotníctva Slovenskej republiky č. 17/2022 o šandardizácii postupu vyšetrenia a zhodnotenia imunohistochemickej expresie proteínu ligandu 1 programovanej smrti v biotických tkanivových vzorkách pacientov so zhubným nádorovým ochorením.

⁴⁶ Epravo.sk, *AI z pohľadu práva*, dostupné na: <https://www.epravo.sk/top/clanky/ai-z-pohladu-prava-4483.html>.

⁴⁷ Zákon č. 40/1964 Zb., Občiansky zákonník v znení neskorších predpisov (ďalej len „Občiansky zákonník“).

⁴⁸ Zákon č. 294/1999 Z. z., o zodpovednosti za škodu spôsobenú vadným výrobkom v znení neskorších predpisov.

- **bezpečnosť výrobkov** – na výrobky, ktorých komponentmi sú systémy umelej inteligencie sa vzťahuje aj súbor **predpisov** upravujúcich uvádzanie výrobkov na trh a ich bezpečnosť, vrátane predpisov tzv. Nového legislatívneho rámca (v tejto súvislosti viď tiež časť 1.3 Štúdie vyššie, ktorá sa týka prepojenia režimu Nariadenia s príslušnými bezpečnostnými predpismi);
- **ochrana spotrebiteľov** - právne predpisy na ochranu spotrebiteľa sa vzťahujú na systémy umelej inteligencie, kedykoľvek sú tieto systémy alebo s nimi súvisiace služby predávané alebo poskytované koncovým spotrebiteľom (vrátane Zákona o ochrane spotrebiteľa⁴⁹); a
- **kybernetickej bezpečnosti** – systémy umelej inteligencie môžu podliehať aj rôznym predpisom z oblasti kybernetickej bezpečnosti v závislosti od systému v rámci ktorého sú využívané alebo v prípade ak sú využívané subjektmi regulovaným týmito predpismi (napr. ak je systém umelej inteligencie súčasťou informačných systémov alebo služieb, na ktoré sa vzťahuje režim Zákona o kybernetickej bezpečnosti).

Len pre doplnenie uvádzame, že k otázke umelej inteligencie sa vyjadril vo svojom náleze⁵⁰ aj Ústavný súd Slovenskej republiky, ktorý rozhodol, že pokiaľ správne orgány (v tomto prípade Finančná správa SR) použijú systémy umelej inteligencie, musí byť zachovaná individuálna kontrola resp. ľudský dohľad nad každým rozhodnutím. Inak povedané, systém umelej inteligencie nesmie výlučne samostatne urobiť rozhodnutie, ktoré bude mať dôsledky pre dotknuté osoby.

Ako bude uvedené podrobnejšie v časti 3.1 vo vzťahu k otázke sandboxov v súčasnosti v prostredí SR takisto neexistuje komplexná právna úprava zastrešujúca ich zriaďovanie a fungovanie, pričom existujúce sandboxy NBS⁵¹ a ÚRSO⁵² nie sú špecificky legislatívne ukotvené s tým, že ich fungovanie je upravené na základe regulačných aktov vydaných v rámci pôsobnosti uvedených orgánov (napr. Pravidlá fungovania regulačného sandboxu NBS). Základný právny rámec pre zriadenie a fungovanie sandboxov pre umelú inteligenciu v kontexte Nariadenia bude zakotvený priamo Nariadením a delegovanými aktmi Komisie.

So zavedením sandboxu resp. sandboxov pre oblasť umelej inteligencie však počíta APDTS - Akčný plán digitálnej transformácie Slovenska na roky 2023 – 2026, schválený vládou SR dňa 14. decembra 2022. Tento dokument definuje ciele SR v oblasti digitalizácie, pričom vymedzuje jednotlivé stratégie vrátane orgánov zodpovedných za ich realizáciu. Súčasťou APDTS je v bode 3.1.1.7 aj opatrenie na vytvorenie experimentálnych regulačných prostredí (sandboxov) pre AI. Ako gestor zodpovedný za realizáciu tohto opatrenia je určené MIRRI (z iniciatívy ktorého bola vypracovaná Štúdia), pričom MIRRI je určené aj ako gestor pre celú oblasť resp. ďalšie opatrenia týkajúce sa umelej inteligencie.⁵³

⁴⁹ Zákon č. 250/2007 Z. z. ochrane spotrebiteľa a o zmene zákona Slovenskej národnej rady č. 372/1990 Zb. o priestupkoch v znení neskorších predpisov (ďalej len „**Zákon o ochrane spotrebiteľa**“).

⁵⁰ Nález Ústavného súdu Slovenskej republiky sp. zn. PL. ÚS 10/2016 z 10. októbra 2018.

⁵¹ Regulačný sandbox NBS, dostupné na: <https://nbs.sk/dohlad-nad-financnym-trhom/fintech/regulacny-sandbox/#prihlaska>.

⁵² Regulačný sandbox ÚRSO, dostupné na: <https://www.urso.gov.sk/regulacny-sandbox/>.

⁵³ MIRRI je v zmysle Kompetenčného zákona ústredný orgán štátnej správy okrem iného pre (i) oblasť investícií v rozsahu strategického plánovania a strategického projektového riadenia, ako aj koordináciu investičných projektov a vypracovanie národného strategického investičného rámca v pôsobnosti MIRRI, a vnútroštátnu implementáciu Agendy 2030 a (ii) centrálné riadenie informatizácie spoločnosti a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní verejných prostriedkov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a koordináciu plnenia úloh v oblasti informatizácie spoločnosti.

3.1.1 Analýza právneho rámca pre implementáciu sandboxov v zmysle požiadaviek Nariadenia a legislatívy SR

V nasledovných častiach pre potreby Štúdie sumarizujeme (i) právny rámec pre sandboxy pre umelú inteligenciu v zmysle Nariadenia (časť 3.1.2 vrátane špecifických požiadaviek na fungovanie sandboxov, a (ii) právny rámec pre ich ukotvenie v slovenskom právnom prostredí (vrátane komparatívneho sumára základných aspektov existujúcich regulačných sandboxov NBS a ÚRSO) (časť 3.1.3.4 Štúdie nižšie).

Zhodnotenie legislatívneho prostredia z pohľadu uskutočniteľnosti zavedenia sandboxu pre umelú inteligenciu v zmysle Nariadenia a odporúčaní v tomto smere je uvedené v časti 3.3 nižšie.

3.1.2 Základný právny rámec pre zriaďovanie sandboxov pre umelú inteligenciu v zmysle Nariadenia

Ako bolo uvedené vyššie, z pohľadu práva EÚ bude základný právny rámec pre zriadenie a fungovanie sandboxov pre umelú inteligenciu v rámci členských štátov EÚ predstavovať (po jeho prijatí) Nariadenie, ktoré v článku 53 ods. 1 zavádza „*povinnosť členských štátov⁵⁴ zriadiť aspoň jedno experimentálne regulačné prostredie pre umelú inteligenciu (sandbox) na vnútroštátnej úrovni*“, ktoré musí byť funkčné najneskôr v deň začatia uplatňovania Nariadenia, pričom toto regulačné prostredie možno zriadiť aj spoločne s jedným alebo viacerými ďalšími členskými štátmi.

Z pohľadu požiadaviek na zriaďovanie a fungovanie sandboxov predpokladaných Nariadením, bude kľúčový aj nadväzujúci delegovaný akt resp. delegované akty Komisie, ktorých vydanie Nariadenie predpokladá (viď čl. 53a Nariadenia), a v ktorých Komisia podrobne opíše spôsoby zriadenia, vývoja, vykonávania a fungovania AI sandboxov a dohľadu nad nimi, vrátane kritérií oprávnenosti a postupu podávania žiadostí, výberu, účasti a opustenia AI sandboxu a práv a povinností účastníkov. Delegované akty by mala Komisia prijať najneskôr do 12 mesiacov od nadobudnutia účinnosti Nariadenia. Aj napriek tomu, že aktuálne nie je k dispozícii znenie delegovaných aktov Komisie, základné požiadavky a modality pre fungovanie sandboxov pre umelú inteligenciu sú rámcovo uvedené v článku 53a Nariadenia a sumarizované v sekcii (i) tejto časti Štúdie nižšie. Pre zriadenie a nastavenie fungovania AI sandboxu v podmienkach Slovenskej republiky tak bude naďalej nevyhnutné sledovať legislatívny proces prijímania delegovaných aktov predpokladaných Nariadením a akékoľvek dodatočné a konkretizované požiadavky z nich vyplývajúce promptne zohľadniť v rámci procesu zriaďovania AI sandboxu v prostredí Slovenskej republiky.

3.1.2.1 Základné požiadavky na fungovanie sandboxov vyplývajúce z Nariadenia z hľadiska povinností členských štátov EÚ a zriaďujúcich orgánov

Medzi hlavné požiadavky na členské štáty EÚ a povinnosti vo vzťahu k zriadeniu a fungovaniu sandboxov vyplývajúce z Nariadenia, ktoré bude potrebné zo strany Slovenskej republiky zohľadniť pri nastavovaní legislatívneho a regulačného prostredia pre AI sandboxy patria nasledovné požiadavky a povinnosti definované Nariadením:

⁵⁴ K eventualite nahradenia uvedenej povinnosti členského štátu, možnosťou zriadenia AI sandboxu viď vysvetlenia vyššie (najmä časť 1.1.1 Štúdie vyššie).

- **zriadenie aspoň jedného sandboxu pre umelú inteligenciu** na vnútroštátnej úrovni, ktorý musí byť funkčný **najneskôr v deň začatia uplatňovania Nariadenia**⁵⁵, pričom sandbox musí poskytnúť kontrolované prostredie, ktoré uľahčí vývoj, testovanie a validáciu inovačných systémov umelej inteligencie na obmedzený čas **pred ich uvedením na trh alebo do prevádzky** podľa konkrétneho plánu dohodnutého medzi potenciálnymi poskytovateľmi a zriaďujúcim orgánom.

S tým súvisí povinnosť zriaďujúceho orgánu prideliť dostatočné (finančné a ľudské)⁵⁶ zdroje na zriadenie a fungovanie AI sandboxu v zmysle požiadaviek Nariadenia;

- **povinnosť nastaviť fungovanie AI sandboxu tak, aby prispel k naplneniu nasledovných základných cieľov:** (a) lepšie chápanie technického vývoja a zlepšenie metód dohľadu na strane zriaďujúcich orgánov;⁵⁷ (b) poskytovať potenciálnym poskytovateľom usmernenia s cieľom dosiahnuť regulačný súlad s Nariadením alebo prípadne inými uplatniteľnými právnymi predpismi EÚ a členských štátov (v prostredí Slovenskej republiky, predpisy Slovenskej republiky); (c) umožniť a uľahčiť potenciálnym poskytovateľom testovanie a vývoj inovačných riešení týkajúcich sa systémov umelej inteligencie; a (d) umožniť regulačné učenie v kontrolovanom prostredí (najmä s cieľom vypracovať lepšie usmernenia a identifikovať možné budúce zlepšenia právneho rámca prostredníctvom riadneho legislatívneho postupu)⁵⁸.
- **povinnosti v oblasti metodiky a dohľadu** na strane orgánu zriaďujúceho AI sandbox a ostatných dotknutých orgánov:
 - poskytovať usmernenia a dohľad v rámci AI sandboxu s cieľom identifikovať riziká, najmä pre základné práva, demokraciu a právny štát, zdravie a bezpečnosť a životné prostredie;
 - testovať a preukazovať zmierňujúce opatrenia pre identifikované riziká a ich účinnosť;
 - zabezpečiť súlad s požiadavkami Nariadenia a prípadne s inými právnymi predpismi EÚ a členských štátov (v prostredí Slovenskej republiky, predpisy Slovenskej republiky); a
 - poskytovať potenciálnym poskytovateľom, ktorí vyvíjajú (najmä) vysokorizikové systémy umelej inteligencie, usmernenia a dohľad nad tým, ako splniť požiadavky stanovené Nariadením, aby systémy umelej inteligencie mohli opustiť AI sandbox s predpokladom zhody s osobitnými požiadavkami Nariadenia, ktoré boli posúdené v rámci AI sandboxu.

Keďže režim Nariadenia pracuje s predpokladom súladu s Nariadením, pokiaľ systém umelej inteligencie spĺňa jeho požiadavky pri opustení experimentálneho prostredia sandboxu, navrhujeme aj v rámci národného legislatívneho nastavenia fungovania AI sandboxu zväziť explicitnú úpravu, aby všetky relevantné orgány dohľadu nad trhom ako aj notifikované osoby (viď najmä časť 2.1.1 vyššie) zohľadňovali správy o výstupoch z AI sandboxu vypracované zriaďujúcim orgánom v kontexte postupov posudzovania zhody alebo kontrol v rámci dohľadu nad trhom;

⁵⁵ T.j. do 2 rokov od nadobudnutia účinnosti Nariadenia.

⁵⁶ Čl. 59 ods. 4 Nariadenia, odôvodnenie (71) Nariadenia.

⁵⁷ Čl. 53 ods. 1e Nariadenia, odôvodnenie (72) Nariadenia.

⁵⁸ Odôvodnenie (72) Nariadenia.

- zabezpečiť, že pokiaľ inovačné systémy umelej inteligencie spracúvajú osobné údaje alebo na inom základe podliehajú dohľadu ďalších vnútroštátnych orgánov alebo príslušných orgánov, ktoré poskytujú alebo podporujú prístup k osobným údajom (v prostredí SR najmä ÚOOÚ), aby vnútroštátne orgány na ochranu údajov alebo v príslušných prípadoch Európsky dozorný úradník pre ochranu údajov (ďalej len „EDPS“)⁵⁹ a ďalšie vnútroštátne orgány boli zapojené v príslušnom rozsahu do prevádzky AI sandboxu a do dohľadu nad jeho aspektmi.

V prostredí SR sa môže z povahy veci jednať najmä o sektorových regulátorov ako napr. NBS a ŠÚKL, pričom umožnenie realizácie metodických a dohľadových právomocí príslušných sektorových regulátorov bude vhodné bez ohľadu na to, či sa v konkrétnom prípade bude jednať o poskytovanie a/alebo podporu prístupu k údajom (viď tiež možnosti nastavenia spolupráce v časti 3.1.3.3 nižšie);

- **základné koordinačné a notifikačné povinnosti** orgánu zriaďujúceho AI sandbox:
 - koordinovať svoje činnosti a spolupracovať s inými zriaďujúcimi orgánmi v rámci Úradu;
 - informovať Úrad o zriadení AI sandboxu s možnosťou požiadať o podporu a usmernenie;
 - predkladať Úradu a Komisii, pokiaľ jediným zriaďujúcim orgánom nie je Komisia, výročné správy so začiatkom rok po zriadení AI sandboxu a potom každý rok až do jeho ukončenia a záverečnej správy;
 - koordinovať aktivity s orgánmi dohľadu na trhu a/alebo notifikovanými osobami a umožniť zapojenie resp. spoluprácu sektorových regulátorov do prevádzky AI sandboxu (viď vyššie);
- **základné požiadavky na právny režim fungovania sandboxu z pohľadu dohľadových právomocí a zodpovednosti potenciálnych poskytovateľov AI systémov** – pri nastavovaní legislatívno-regulačného rámca fungovania sandboxu v rámci Slovenskej republiky bude nevyhnutné zabezpečiť súlad s nižšie uvedenými základnými princípmi vyplývajúcimi z čl. 53 ods. 3 a ods. 4 Nariadenia:
 - právomoci príslušných orgánov v oblasti dohľadu a nápravy nebudú fungovaním sandboxu pre umelú inteligenciu dotknuté (a to aj na regionálnej a miestnej úrovni).

Akékoľvek významné riziká pre základné práva, demokraciu, právny štát, zdravie, bezpečnosť alebo životné prostredie, ktoré sa zistia počas vývoja a testovania systémov umelej inteligencie, musia mať za následok okamžité a primerané zmiernenie rizík. Príslušné orgány musia mať právomoc dočasne alebo natrvalo pozastaviť testovanie alebo účasť v AI sandboxe, ak nie je možné účinné zmiernenie, a o takomto rozhodnutí informujú Úrad.
 - Potenciálni poskytovatelia budú (podľa uplatniteľných právnych predpisov týkajúcich sa zodpovednosti)⁶⁰ zodpovední za akúkoľvek škodu spôsobenú tretím stranám v dôsledku experimentov, ktoré sa budú v AI sandboxe uskutočňovať.

Ak však potenciálni poskytovatelia budú (a) dodržiavať konkrétny plán (v zmysle čl. 53 ods. 1c Nariadenia) a podmienky svojej účasti a (b) v dobrej viere sa budú riadiť usmerneniami zriaďujúceho orgánu, orgán neprijme žiadne administratívne donucovacie opatrenia za porušenie Nariadenia.

⁵⁹ Pokiaľ ide o experimentálne regulačné prostredie pre umelú inteligenciu na úrovni Únie, do prevádzky a dohľadu zapojí európsky dozorný úradník pre ochranu údajov

⁶⁰ Vrátane slovenského predpisu/predpisov implementujúcich Smernicu o zodpovednosti.

3.1.2.2 Základné modalitty a požiadavky na fungovanie sandboxu pre umelú inteligenciu v prostredí Slovenskej republiky v zmysle Nariadenia

Z požiadaviek na modalitty a fungovanie AI sandboxov uvádzaných v čl. 53a a 54a⁶¹ Nariadenia vyplýva, že AI sandboxy zriaďované členskými štátmi (vrátane Slovenskej republiky) budú musieť spĺňať najmä nasledovné kritériá, ktoré sú následne zohľadnené aj v rámci odporúčaní pre zriadenie AI sandboxu v časti 3.3.1. Štúdie nižšie:

- sandbox by mal byť schopný prispôbiť sa **fyzickým** aj **virtuálnym** produktom;⁶²
- sandbox musí byť **otvorený každému žiadajúcemu potenciálnemu poskytovateľovi** systému umelej inteligencie, **ktorý spĺňa kritériá** oprávnenosti a výberu;
- kritériá prístupu do sandboxu musia byť **transparentné a spravodlivé** a zriaďujúci orgán informuje žiadateľov o svojom rozhodnutí **do 3 mesiacov** od podania žiadosti;
- sandboxy musia umožňovať **široký a rovnaký prístup** a udržiavať krok s dopytom po účasti;
- prístup k experimentálnym regulačným prostrediam pre umelú inteligenciu musí byť **pre MSP a startupy bezplatný** bez toho, aby boli dotknuté mimoriadne náklady, ktoré môže zriaďujúci orgán vymáhať spravodlivým a primeraným spôsobom;
- sandbox musí uľahčovať zapojenie ďalších relevantných aktérov v rámci ekosystému umelej inteligencie (viď aj okruh dotknutých subjektov v časti 2.1.2 Štúdie vyššie);
- sandbox musí umožniť potenciálnym poskytovateľom v riadenom prostredí **splniť povinnosti posudzovania zhody** podľa Nariadenia alebo dobrovoľné uplatňovanie kódexov správania v zmysle čl. 69 Nariadenia;
- postupy, procesy a administratívne požiadavky na podávanie žiadostí, výber, účasť a odchod z AI sandboxu musia byť jednoduché, ľahko zrozumiteľné, jasne komunikované s cieľom uľahčiť účasť MSP a startupov s obmedzenými právnymi a administratívnymi kapacitami, a aby boli zosúladené v celej EÚ, a tak sa zabránilo fragmentácii, a aby sa účasť v AI sandboxe vytvorenom členským štátom (SR), Komisiou alebo EDPS vzájomne a jednotne uznávala a mala rovnaké právne účinky v celej EÚ;
- účasť na AI sandboxe musí byť **obmedzená na obdobie, ktoré je primerané zložitosti a rozsahu projektu**;
- AI sandbox musí uľahčovať vývoj nástrojov a infraštruktúry na testovanie, referenčné porovnávanie, posudzovanie a vysvetľovanie rozmerov systémov umelej inteligencie relevantných pre sandboxy, ako sú presnosť, spoľahlivosť a kybernetická bezpečnosť, ako aj minimalizácia rizík v oblasti základných práv, životného prostredia a spoločnosti ako celku;
- potenciálnym poskytovateľom v AI sandboxoch, najmä **MSP a startupom, sa musí uľahčiť prístup k službám pred nasadením**, ako sú usmernenia týkajúce sa vykonávania Nariadenia, k iným službám s pridanou hodnotou, ako je pomoc s normalizačnými dokumentmi a certifikáciou a konzultácie, a k iným iniciatívam digitálneho jednotného trhu, ako sú testovacie a experimentálne zariadenia, digitálne centrá, centrá excelentnosti a možnosti referenčného porovnávania EÚ;

⁶¹ Čl. 54a Nariadenia - Presadzovanie výskumu a vývoja umelej inteligencie na podporu sociálne a environmentálne prospešných výsledkov.

⁶² Odôvodnenie (71) Nariadenia.

- AI sandbox musí umožňovať **prednostný prístup relevantným projektom podporujúcim sociálne a environmentálne prospešné výsledky**, pokiaľ spĺňajú definované podmienky oprávnenosti, okrem iného vrátane riešení založených na umelej inteligencii s cieľom zvýšiť prístupnosť pre osoby so zdravotným postihnutím, riešiť sociálno-ekonomické nerovnosti a splniť ciele v oblasti udržateľnosti a životného prostredia⁶³;
- v prípade potreby by mal byť aj v rámci AI sandboxu vytvorený dostupný vyhradený kanál na komunikáciu s projektmi s cieľom poskytovať usmernenia a odpovedať na otázky týkajúce sa vykonávania Nariadenia; a
- prípadné ďalšie modalitty, ktoré budú vyplývať z finálneho textu Nariadenia a/alebo delegovaných aktov.

Nariadenie zároveň stanovuje bližšie podmienky spracúvania osobných údajov v kontexte prevádzkovania AI sandboxu (čl. 54 Nariadenia), pričom nižšie uvádzame tie, ktoré považujeme z pohľadu nastavenia fungovania sandboxu za najdôležitejšie:

- Nariadenie umožňuje v prípade osobných údajov, ktoré boli pôvodne zozbierané prevádzkovateľom na iné účely spracúvanie aj v rámci AI sandboxu, avšak vyžaduje sa kumulatívne splnenie: **(a) osobitného účelu**: osobné údaje je možné spracúvať výlučne za osobitným účelom ochrany významného verejného záujmu špecifikovaným v Nariadení; a **(b) ďalších podmienok stanovených Nariadením**, najmä:
 - všetky osobné údaje určené na spracovanie v rámci AI sandboxu musia byť umiestnené vo funkčne oddelenom, izolovanom a bezpečnom procesnom prostredí pod správou príslušných poskytovateľov. Prístup k týmto údajom je obmedzený iba na osoby s oprávnením;
 - spracúvanie osobných údajov nesmie mať žiadny vplyv na dotknuté osoby;
 - spracúvané osobné údaje sú chránené primeranými technickými a organizačnými opatreniami a po skončení doby ich zákonného uchovávaní budú trvalo vymazané;
 - logy zo spracúvania osobných údajov sa uchovávajú iba po dobu trvania účasti v AI sandboxe.

3.1.3 Základný právny rámec a požiadavky na zavedenie AI sandboxu predpokladaného Nariadením v zmysle slovenskej legislatívy a prehľad možných alternatív

Ako už bolo uvedené vyššie, v súčasnosti v právnom prostredí Slovenskej republiky neexistuje komplexná legislatívna úprava pôsobnosti regulačných sandboxov, či už vo vzťahu k úprave právneho základu zriaďovania sandboxov (vo vzťahu k systémom umelej inteligencie alebo iným riešeniam) a/alebo stanovenia konkrétnych požiadaviek na ich fungovanie, pričom aj aktuálny režim fungovania existujúcich sandboxov NBS a ÚRSO nevychádza z jednotného legislatívneho základu a líši sa tak čo sa týka formy aj obsahu (viď sekciu (iii) tejto časti Štúdie nižšie). Rovnako ani Nariadenie aktuálne neupravuje konkrétny postup ani formu, ktorou má byť sandbox (resp. sandboxy) pre umelú inteligenciu (v zmysle požiadaviek Nariadenia) zriadený v prostredí konkrétneho členského štátu EÚ.

⁶³ Viď čl. 54a Nariadenia.

S prihliadnutím na uvedené teda Slovenská republika (i) má v tomto smere má značnú voľnosť akým spôsobom ciele a požiadavky Nariadenia vo vzťahu k zriadeniu a fungovaniu AI sandboxu naplní (pri rešpektovaní požiadaviek na fungovanie AI sandboxu stanovených Nariadením) a (ii) môže si vybrať najvhodnejší spôsob zohľadňujúci okrem iného preferovanú štruktúru inštitucionálneho rámca pre aplikáciu Nariadenia (viď aj časť 2.1.1 vyššie).

Z analýzy existujúceho právneho rámca máme tiež za to, že v súčasnosti neexistujú materiálne legislatívne prekážky pre zriadenie a fungovanie AI sandboxu predpokladaného Nariadením. To potvrdzuje aj aktuálne pôsobenie regulačných sandboxov NBS a ÚRSO v právnom prostredí Slovenskej republiky. Na druhej strane konkrétne špecifiká pre zriadenie a fungovanie AI sandboxu a výber najvhodnejšieho riešenia budú závisieť aj od toho akým spôsobom budú implementované požiadavky Nariadenia najmä vo vzťahu k inštitucionálnemu rámcu predpokladanému Nariadením do existujúceho právneho a inštitucionálneho rámca Slovenskej republiky (najmä čo sa týka určenia príslušného vnútroštátneho dozorného orgánu a orgánu zriaďujúceho AI sandbox a nastavenia spolupráce s inými OVM).

V tejto súvislosti považujeme za najdôležitejšie nasledovné aspekty, ktoré budú mať vplyv na rozsah legislatívnej a administratívnej náročnosti celkového procesu, a ktoré bude potrebné zvážiť na strane príslušných OVM SR (a to aj s prihliadnutím na závery a odporúčania TSI Analýzy):

- **určenie príslušného vnútroštátneho dozorného orgánu** – viď časť 2.1.1 Štúdie vyššie), v ktorého kompetencii bude agenda uplatňovania Nariadenia, vrátane alebo bez zahrnutia zriadenia AI sandboxu, pričom medzi základné alternatívy patrí:

- a. **kreovanie nového vnútroštátneho dozorného orgánu** (napr. ako v prípade Španielska – viď časť 3.2.1 Štúdie); alebo
- b. **rozšírenie kompetencií niektorého z existujúcich OVM** za účelom zefektívnenia procesu kreovania inštitucionálneho rámca a využitia existujúcich kapacít.

V súvislosti so zriadením sandboxu pre umelú inteligenciu predpokladaného Nariadením sa s prihliadnutím na systematické a praktické aspekty uvedeného riešenia javí ako vhodné zvážiť zaradenie zriadenia AI sandboxu do pôsobnosti už existujúceho OVM, ktorý bude určený Slovenskou republikou ako vnútroštátny dozorný orgán v zmysle Nariadenia, a ktorý pre tieto účely bude môcť (okrem iného) využiť aj svoje existujúce kapacity, ak nebudú identifikované dôvody, pre ktoré by mal byť zriaďujúcim orgánom AI sandboxu iný OVM SR.

Medzi ďalšie aspekty podporujúce dané riešenie patrí najmä (i) predpokladaná pôsobnosť vnútroštátneho dozorného orgánu v oblasti vydávania usmernení a poradenstva týkajúceho sa vykonávania Nariadenia (čl. 59 ods. 7 Nariadenia) a dohľadu a kontroly v oblasti pôsobnosti Nariadenia, a (ii) možnosť priameho využívania diskrečnej právomoci daného orgánu pri posudzovaní záležitostí súvisiacich s prevádzkovaním AI sandboxu, vrátane neuplatnenia donucovacích opatrení za porušenie Nariadenia účastníkmi AI sandboxu (viď čl. 53 ods. 4 Nariadenia a časť 3.1.3.1 Štúdie vyššie);

- **stanovenie konkrétnej legislatívno-technickej formy zriadenia a zakotvenia sandboxu pre umelú inteligenciu** v slovenskom právnom prostredí pri zohľadnení základných regulačných princípov pre zriadenie a fungovanie sandboxu (v tejto súvislosti viď najmä sekciu (ii) tejto časti Štúdie nižšie) a ďalších tzv. best practices vyplývajúcich z benchmarkingu sumarizovaných v ďalších častiach Štúdie (viď najmä časť 3.2.1 a 3.1.3.4 Štúdie nižšie);

- nastavenie štruktúry a vzťahov spolupráce vnútroštátneho dozorného orgánu resp. (primárneho) orgánu zriaďujúceho AI sandbox a ostatných dotknutých OVM vo vzťahu k fungovaniu AI sandboxu z legislatívneho a praktického pohľadu - vid' sekcia 3.1.3.3 tejto časti Štúdie nižšie.

3.1.3.1 Legislatívno-technické možnosti zavedenia sandboxu pre umelú inteligenciu v Slovenskej republike

Z legislatívno-technického pohľadu je možné uvažovať o viacerých formách úpravy zriadenia AI sandboxu predpokladaného Nariadením v právnom prostredí SR, vrátane:

- a. použitia tzv. doložiek o experimentálnom režime/experimentálnych doložiek** (t.j. zákonná úprava napr. formou vloženia príslušných zákonných ustanovení upravujúcich základný rámec fungovania AI sandboxu do zákona zavádzajúceho právomoci vnútroštátneho dozorného orgánu)⁶⁴
Pozn. doložky o experimentálnom režime⁶⁵ sú tiež uvádzané ako jeden z hlavných nástrojov adaptívnej regulácie vhodných pre použitie pri regulácii inovatívnych technológií v dokumente Komisie „Better regulation toolbox“ (vydanie z júla 2023)⁶⁶ – v tomto dokumente je ako príklad doložky o experimentálnom režime uvádzaný napr. článok 39 Nariadenia EÚ o schvaľovaní motorových vozidiel⁶⁷;
- b. úpravy fungovania AI sandboxu primárne podzákonnými normatívnymi alebo inými regulačnými aktmi** napr. vo forme tzv. soft-law a/alebo iných aktov vydaných v rámci kompetencie príslušných OVM (ako napr. Pravidlá fungovania regulačného sandboxu NBS);
- c. využitím existujúceho resp. budúceho právneho režimu (po prijatí národnej legislatívy implementujúcej požiadavky Nariadenia) bez zavedenia doložiek o experimentálnom režime s primárnym uplatňovaním diskrečnej právomoci príslušného orgánu resp. orgánov, v rámci ich právomoci; a/alebo**
- d. kombináciou predchádzajúcich možností.**

⁶⁴ V zmysle "Záverov Rady o experimentálnych regulačných prostrediach a doložkách o experimentálnom režime ako o nástrojoch pre nadčasový a odolný regulačný rámec priaznivý pre inováciu, ktorý zvláda zlomové výzvy v digitálnom veku" (2020/C 447/01) (ďalej len „**Závery Rady**“) sú **doložky o experimentálnom režime** „*právne ustanovenia, ktoré umožňujú orgánom povereným vykonávaním a presadzovaním právnych predpisov uplatňovať v jednotlivých prípadoch určitý stupeň flexibility v súvislosti s testovaním inováčných technológií, výrobkov, služieb alebo prístupov*“. V Záveroch Rady sa tiež uvádza, že doložky o experimentálnom režime sú „*často právnym základom pre experimentálne regulačné prostredia a už sa používajú v právnych predpisoch EÚ a v právnych rámcoch mnohých členských štátov*“ (podčiarknutie doplnené).

⁶⁵ V zmysle daného dokumentu „doložka o experimentálnom režime“ umožňuje orgánom povereným aplikáciou a presadzovaním právnych predpisov uplatniť určitý stupeň flexibility vo vzťahu k inovatívnym technológiám, produktom alebo prístupom, aj keď nespĺňajú všetky existujúce zákonné požiadavky.

⁶⁶ Dostupné na: <https://commission.europa.eu/system/files/2023-09/BR%20toolbox%20-%20Jul%202023%20-%20FINAL.pdf>

⁶⁷ Článok 39 Nariadenia EÚ o schvaľovaní motorových vozidiel (Výnimky pre nové technológie alebo nové koncepcie) umožňuje členským štátom na základe povolenia Komisie schváliť technológie alebo koncepcie, aj keď nespĺňajú určité požiadavky. Kým sa čaká na rozhodnutie Komisie o tom, či výnimku povolí, členský štát môže udeliť dočasné povolenie, ktoré je platné len na jeho území.

S prihliadnutím na (i) komplexnosť a prierezovosť požiadaviek na zriadenie a fungovanie AI sandboxov v zmysle Nariadenia, (ii) potrebu implementácie požiadaviek Nariadenia do slovenského právneho poriadku⁶⁸, v súvislosti s ktorou bude (bez ohľadu na problematiku AI sandboxov) potrebná komplexná legislatívna úprava formou vydania nového zákona a/alebo novelizácie aktuálnych zákonov, v rámci ktorej bude možnosť základnej úpravy fungovania AI sandboxu na zákonnej úrovni (okrem iného po zohľadnení záverov a odporúčaní TSI Analýzy), ako aj (iii) aj pre zabezpečenie právnej istoty a robustnosti legislatívneho ukotvenia AI sandboxu, sa v aktuálnej fáze javí ako vhodné zvážiť pre zriadenie AI sandboxu využitie kombinácie vyššie uvedených postupov, a to najmä zakotvenie právneho rámca pre fungovanie AI sandboxu formou zákonnej doložky o experimentálnom režime s konkrétnejšou reguláciou praktických aspektov fungovania AI sandboxu (najmä pravidiel prihlasovania, hodnotenia kritérií a pod.) formou iných vykonávacích regulačných aktov príslušných orgánov umožňujúcich vyššiu flexibilitu reagovania na prípadné zmeny alebo požiadavky súvisiace s fungovaním AI sandboxu.

Odhliadnuc od sandboxov NBS a ÚRSO, ktoré neboli zriaďované formou osobitnej zákonnej úpravy (viď sekcia 3.1.3.4 nižšie), je v tejto súvislosti možné pre porovnanie uviesť režim zavádzania prioritizačnej politiky⁶⁹ a záväzkov⁷⁰ v kompetencii Protimonopolného úradu SR (ďalej len „PMÚ“), pričom právomoc PMÚ vydať prioritizačnú politiku a riešiť identifikované porušenie ZOHS⁷¹ formou záväzkov úpravy správania (a nie uložením sankcie) je primárne ukotvená v ZOHS (viď ustanovenia § 16 ods. 1 písm. j), § 16 ods. 2, § 33 ZOHS), pričom podrobnosti týchto opatrení sú následne upravené regulačnými aktmi PMÚ a aplikované v rámci diskrečnej právomoci PMÚ.

⁶⁸ Okrem iného za účelom určenia vnútroštátneho dozorného orgánu s príslušnými právomocami na uplatňovanie Nariadenia.

⁶⁹ Prioritizačná politika sa opiera o pravidelne aktualizované prioritizačné kritériá, pričom ich cieľom je stanoviť účelný a transparentný postup selekcie a vyhodnotenia prípadov, v ktorých PMÚ začne konať. Cieľom prioritizácie pritom je efektívne alokovať zdroje PMÚ na činnosti, ktoré zabezpečia zásah v tých prípadoch, v ktorých dochádza k najvýznamnejším obmedzeniam hospodárskej súťaže. Viď. Priorizačná politika úradu, aktualizované 24. augusta 2022, dostupné na: <https://www.antimon.gov.sk/priorizacna-politika-uradu/?csrt=9125454553723911081>.

⁷⁰ Viď. Záväzky, úprava postupu Protimonopolného úradu SR podľa § 33 zákona, dostupné na: https://www.antimon.gov.sk/data/files/1214_zavazky-uprava-postupu-protimonopolneho-uradu-sr-podla-%C2%A7-33-zakona.pdf?csrt=10984890789242975246

⁷¹ Zákon č. 187/2021 Z. z. o ochrane hospodárskej súťaže a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „ZOHS“).

3.1.3.2 Základné princípy regulačného ukotvenia sandboxu pre umelú inteligenciu

Bez ohľadu na konkrétny režim zavedenia AI sandboxu, máme za to, že akýkoľvek zvolený režim bude musieť spĺňať základné právne princípy regulačnej politiky, ktoré musia vždy rešpektovať a mali by podporovať uplatňovanie najmä zásad (i) legality⁷², (ii) proporcionality⁷³, (iii) transparentnosti⁷⁴, (iv) subsidiarity⁷⁵, (v) predvídateľnosti a právnej istoty⁷⁶, a (vi), ako aj zásady predbežnej opatrnosti⁷⁷.

Rovnako je v tejto súvislosti vždy potrebné zabezpečiť aj vysokú úroveň ochrany občanov, spotrebiteľov, zamestnancov, zdravia, klímy a životného prostredia, a nielen ich, ako aj právnu istotu, finančnú stabilitu, rovnaké podmienky a spravodlivú hospodársku súťaž, pričom treba rešpektovať aj existujúcu úroveň ochrany.⁷⁸ Máme za to, že rámcovo tieto princípy boli zohľadnené aj pri definovaní modalít fungovania AI sandboxov v ustanoveniach Nariadenia (najmä kritériá uvádzané v čl. 53a Nariadenia) a mali by byť zohľadnené pri zavádzaní AI sandboxu v prostredí SR.

Čo sa týka ďalších konkrétnych požiadaviek na legislatívne zavedenie príslušnej doložky o experimentálnom režime (ako aj ostatných alternatív uvedených vyššie) v súvislosti so zriaďovaním sandboxu predpokladaného

⁷² V zmysle tohto princípu OVM nie sú oprávnené konať, ak ich na to nespĺnomocní zákon, a ak konajú, sú povinné konať iba spôsobom, ktorý ustanovil zákon (viď napr. DRGONEC, Ján. Ústava Slovenskej republiky. 2. vydanie. Bratislava: C. H. Beck, 2019).

⁷³ Tento princíp okrem iného zahŕňa požiadavku, aby OVM pri svojom postupe neprekračovali hranice toho, čo je vhodné a potrebné na dosiahnutie sledovaných cieľov, čím sa rozumie, že v prípade, kde existuje voľba medzi viacerými primeranými opatreniami, je potrebné prikloniť sa tomu najmenej obmedzujúcemu (obdobne viď aj prístup Úradu pre verejné obstarávanie v rámci metodických usmernení vo svojej pôsobnosti).

⁷⁴ Princíp transparentnosti v tomto ohľade znamená okrem iného predvídateľnosť konania OVM zo strany kontrolných orgánov, pričom zabezpečuje pre dotknuté subjekty adekvátny stupeň zverejnenia, ktorý umožňuje otvorený a nediskriminačný prístup do AI sandboxu, ako aj následnú kontrolu nestrannosti postupov a procesných úkonov s tým spojených. Cieľom princípu transparentnosti, ktorý dopĺňa princíp rovnakého zaobchádzania, je zabrániť riziku uprednostňovania určitých záujemcov a svojvoľného prístupu OVM (viď obdobne aj, SIMINSKÁ, E., Mgr., Rozhodnutia úradu na ochranu hospodárskej súťaže v oblasti verejného obstarávania v zdravotníctve, Právo a manažment v zdravotníctve 6/2023).

⁷⁵ V zmysle princípu subsidiarity je najmä potrebné zaručiť stupeň nezávislosti rozhodovania nižšieho orgánu prevádzkujúceho AI sandbox vo veciach prevádzky sandboxu vo vzťahu k vyššiemu orgánu (viď napr. <https://www.europarl.europa.eu/factsheets/sk/sheet/7/the-principle-of-subsidiarity>).

⁷⁶ Princíp predvídateľnosti rozhodovania a rozhodnutia znamená, že účastníci právnych vzťahov môžu legitímne očakávať, že štátne orgány budú v skutkovo a právne porovnateľných prípadoch rozhodovať rovnako. Iba takýto postup rešpektuje princíp právnej istoty a jeho dôsledné dodržiavanie sa významne pozitívne prejavuje aj v rámci celkového nazerania spoločnosti na význam a úlohu práva. (viď Nález Ústavného súdu Slovenskej republiky sp. zn. III. ÚS 275/2018 z 25. júna 2019).

⁷⁷ Zásadou predbežnej opatrnosti sa rozumie taký prístup k riadeniu rizík, podľa ktorého by sa istá politika či isté opatrenie nemali vykonávať, ak existuje možnosť, že politika alebo opatrenie môžu privodiť škodu verejnosti či životnému prostrediu, a ak ešte v tejto otázke nebola dosiahnutá vedecká zhoda. Politiku alebo opatrenie je možné prehodnotiť, keď bude k dispozícii viac vedeckých informácií. Zásada predbežnej opatrnosti sa vymedzuje v článku 191 Zmluvy o fungovaní Európskej únie (ZFEÚ) ako zásada predchádzania škodám. Viď. https://eur-lex.europa.eu/legal-content/EN-SK/TXT/?from=EN&uri=LEGISSUM%3Aprecautionary_principle

⁷⁸ V tejto súvislosti viď tiež bod 12 Záverov Rady.

Nariadením, nad rámec základných princípov uvedené vyššie a legislatívnych pravidiel vyplývajúcich primárne z Legislatívnych pravidiel vlády SR⁷⁹ (ktoré na tomto mieste detailne nerozoberáme) považujeme za potrebné poukázať na nižšie uvedené zahraničné štandardy na obsah experimentálnej doložky, ktorých zohľadnenie v relevantnom rozsahu je možné odporučiť aj pri zriaďovaní AI sandboxu v SR⁸⁰:

- a. **definovanie príslušnosti a právomoci konkrétneho orgánu resp. orgánov vo veciach AI sandboxu (napr. vnútroštátny dozorný orgán - vid' vysvetlenia vyššie)** – určenie orgánu, ktorý rozhoduje o tom, či a ako možno vykonať testovanie inovácie a či je možné sa na tento účel odchýliť od zákonných požiadaviek (**pozn.** vo všeobecnosti by to mal byť príslušný kompetentný orgán, ktorý má hlboké znalosti v príslušnej oblasti – v tomto prípade oblastí relevantných pre reguláciu umelej inteligencie, inovatívnych technológií a pod.).

Ak sa prekrývajú kompetencie viacerých orgánov, je potrebné zvážiť, či musia byť alebo by mali byť zapojené aj iné OVM. Toto zapojenie môže prebiehať jednoduchou formou, napr. prostredníctvom konzultácie, koordinácie aktivít (napr. formou dohôd o spolupráci - vid' tiež sekcia (iii) nižšie) alebo v odôvodnených prípadoch, zakotvením potreby (predchádzajúceho) súhlasu a/alebo inej formy ingerencie daného orgánu v zákone;

- b. **splnomocnenie príslušného orgánu na vydávanie rozhodnutí vo veciach AI sandboxu** – splnomocnenie môže mať rôzne formy napr. (a) zakotvenie povinnosti vydať súhlas/povolenie (napr. na testováciu prevádzku), potom, čo potenciálny poskytovateľ splní stanovené požiadavky, alebo (b) zakotvenie možnosti vydať súhlas/povolenie na základe úvahy orgánu, a **definovanie typu rozhodnutí a/alebo iných aktov (a ich rozsahu), ktoré môže orgán vydať** najmä vydanie súhlasu alebo povolenia a/alebo udelenie výnimky z určitých povinností bez udelenia povolenia alebo zákonné splnomocnenie orgánu upraviť udelenie výnimiek na základe vykonávacích aktov;
- c. **definovanie rozsahu riešení, ktoré sa môžu zapojiť do sandboxu a/alebo benefitovať z regulačných výhod s tým spojených** – rozsah musí byť formulovaný tak, aby existovala primeraná rovnováha medzi špecifickosťou a flexibilitou, pričom špecifickosť zabezpečuje právnu istotu a flexibilita efektívnosť rozhodovania (vydávané rozhodnutia/akty majú byť transparentné a vydávané na základe prijateľných, a spoľahlivých kritérií);
- d. **definovanie materiálnych obmedzení účasti v sandboxe** – účelom je vyváženie výhod testovania s protichodnými záujmami a obavami - obmedzí sa účasť inovácií (AI systémov), ktorých testovanie nie je opodstatnené, pretože by napr. zahŕňalo značné riziká, t. j. ktoré preto nie sú vhodné na testovanie a/alebo sa špecifikuje rozsah, v rámci ktorého je testovanie opodstatnené;

⁷⁹ Legislatívne pravidlá vlády Slovenskej republiky.

⁸⁰ Pri identifikácii týchto štandardov sme vychádzali primárne z požiadaviek na zavádzanie regulačných experimentálnych doložiek v Nemecku, ktoré považujeme vo veľkej miere za aplikovateľné aj v prostredí Slovenskej republiky. Vid' najmä dokument „New flexibility for innovation, Guide for formulating experimentation clauses“ vydaný nemeckým Federálnym ministerstvom pre ekonomické záležitosti a energetiku (BMW) z decembra 2020 dostupný na: https://www.bmw.de/Redaktion/EN/Publikationen/Digitale-Welt/guide-new-flexibility-for-innovation-en-web-bf.pdf?__blob=publicationFile&v=1

- e. **definovanie procesných pravidiel účasti v sandboxe** – v prípadoch, keď sa od záujemcov/potenciálnych poskytovateľov bude vyžadovať predloženie žiadosti o účasť v sandboxe, je potrebné na strane príslušného orgánu stanoviť pravidlá podávania žiadostí, pričom tieto pravidlá nemusia byť nevyhnutne zahrnuté do samotnej textácie zákonného ustanovenia (doložky o experimentálnom režime), ak budú definované v iných aktoch upravujúcich fungovanie sandboxu (zákonné ustanovenie by však malo obsahovať splnomocnenie na vydanie takýchto aktov);
- f. **určenie súvisiacich povinností pre účastníkov sandboxu (resp. oprávnenie stanoviť uvedené povinnosti)** – pre zabezpečenie ochrany tretích strán najmä vo vysoko rizikových oblastiach a na vyhodnotenie účinnosti sandboxu, je potrebné zakotviť možnosť ukladať sprievodné povinnosti súvisiace s účasťou v sandboxe najmä povinnosti monitorovania alebo podávania správ alebo povinnosť zúčastňovať sa na vedeckých štúdiách. Keďže sprievodné povinnosti môžu zasahovať do základných práv zúčastnených subjektov, musia byť opodstatnené a primerané a ich rozsah musí vychádzať z povinnosti chrániť oprávnené záujmy v súvislosti s testovaním;
- g. **stanovenie konkrétnych časových limitov na testovanie** – časové limitácie na testovanie je potrebné stanoviť tak, aby bol jasný dočasný účel testovania, ale aby bol k dispozícii dostatok času na testovanie a súvisiaci proces regulačného učenia na strane príslušného orgánu (k časovým aspektom existujúcich sandboxov vid' napr. časť 3.2.1). Trvanie časového limitu môže byť štruktúrované rôznym spôsobom napr. ponechaním možnosti stanoviť časový limit na orgáne zriaďujúcom sandbox, definovaním konkrétneho času v zmysle Nariadenia (s/bez možnosti predĺženia) a pod.;
- h. **úprava procesu hodnotenia pôsobenia sandboxu** – aby testovanie inovácií v rámci sandboxu mohlo viesť k regulačnému učeniu, sa typicky stanovuje proces hodnotenia úspešnosti dosahovania cieľov sandboxu, najmä za účelom poskytnutia informácií o tom, či a do akej miery sa dosahujú ciele sandboxu, ako je potrebné ho zlepšiť, a či a do akej miery možno získané poznatky preniesť do bežnej praxe;
- i. **zavedenie splnomocňujúcich ustanovení na vydávanie vykonávacích (podzákonných) predpisov a iných aktov** umožňujúcich flexibilne reagovať na praktické situácie súvisiace s fungovaním sandboxu – použitie vykonávacích predpisov alebo inej formy (podzákonných alebo soft law) regulačných aktov, sa odporúča najmä tam, kde je potrebné flexibilne formulovať prvky zamerané na zníženie rizika, napr. procesné požiadavky, vecné obmedzenia súvisiace s účasťou na sandboxe, rozsah alebo sprievodné povinnosti súvisiace s testovaním. Výhodou možnosti úpravy prostredníctvom týchto aktov je to, že sa pravidlá sandboxu dajú ľahšie meniť, ak sa kľúčové predpoklady, ako napríklad hodnotenie rizík, v priebehu testovania zmenia;
- j. medzi ďalšie náležitosti, ktoré je možné v rámci experimentálnej doložky konkrétnejšie upraviť patria najmä: (i) stanovenie účelu a rozsahu testovania, (ii) dodatočné sprievodné obmedzenia (napr. určité obmedzenia/povinnosti vzťahujúce sa na účastníkov sandboxu), (iii) možnosť predčasného odobratia súhlasu alebo povolenia vydaného príslušným dozorným orgánom v kontexte prevádzkovania sandboxu, a (iv) stanovenie časového limitu účinnosti experimentálnej doložky.

3.1.3.3 Možnosti nastavenia štruktúry a vzťahov spolupráce vnútroštátneho dozorného orgánu resp. (primárneho) orgánu zriaďujúceho sandbox a ostatných dotknutých OVM vo vzťahu k fungovaniu sandboxu

Ako už bolo uvedené vyššie (viď časť 2.1.1 Štúdie vyššie) Nariadenie predpokladá zriadenie resp. nastavenie komplexného inštitucionálneho rámca, pričom aj do procesu fungovania AI sandboxu bude zapojených viacero OVM s kompetenciami v príslušných sektorových záležitostiach. Optimálne nastavenie spolupráce daných OVM v slovenskom prostredí bude v značnej miere závisieť od preferovaného usporiadania, ktoré bude výsledkom ďalšieho hodnotenia okrem iného v nadväznosti na závery a odporúčania TSI Analýzy.

Vo všeobecnosti tomto ohľade prichádza do úvahy najmä možnosť úpravy základného rámca spolupráce dotknutých OVM legislatívnou úpravou v rámci doložky o experimentálnom režime (viď najmä bod a. sekcie 3.1.3.1 vyššie). Podporne je možné tiež uvažovať o úprave konkrétnych vzťahov formou dohody resp. dohôd o spolupráci medzi OVM⁸¹ v zmysle § 38 ods. 5 Kompetenčného zákona⁸² s prípadným riešením potenciálnych kompetenčných sporov okrem iného v rámci režimu predpokladaného Správnym súdnym poriadkom.⁸³

3.1.3.4 Komparatívny prehľad základných aspektov existujúcich regulačných sandboxov NBS a ÚRSO

Pre účely porovnania a poukázania na určité aspekty fungovania dvoch regulačných sandboxov, ktoré aktuálne fungujú v rámci SR, a vo vzťahu ku ktorým navrhujeme určité modifikácie pri kreovaní AI sandboxu v zmysle Nariadenia, v nižšie uvedenej tabuľke sumarizujeme základné prvky fungovania regulačných sandboxov NBS a ÚRSO.

⁸¹ Viď napr. Dohoda o spolupráci medzi Protimonopolným úradom Slovenskej republiky a Úradom pre verejné obstarávanie marec 2018, dostupné na:

https://www.antimon.gov.sk/data/files/912_s-uradom-pre-verejne-obstaravanie-marec-2018.pdf?csrt=9125454553723911081, Dohoda o vzájomnej spolupráci medzi Národnou bankou Slovenska a Ministerstvom vnútra Slovenskej republiky, dostupné na:

https://nbs.sk/_img/documents/dohlad/orm/aml/2013_11_29_konecna_verzia_dohody_bez_priloh.pdf, Dohoda o spolupráci medzi Úradom vlády Slovenskej republiky a Úradom pre verejné obstarávanie, dostupné na: https://www.crz.gov.sk/data/att/1956641_dokument1.pdf

⁸² V zmysle § 38 ods. 5 Kompetenčného zákona „[na] účely zabezpečenia efektívnejšieho výkonu jednotlivých činností môžu ministerstvá a ostatné ústredné orgány štátnej správy uzavrieť písomnú dohodu o spolupráci, v ktorej sa vymedzí najmä druh a rozsah vykonávaných činností spolupráce.“ Medzi príklady takýchto dohôd v praxi patria: Dohoda o spolupráci, zmluva o spolupráci, memorandum o spolupráci, dohoda o vzájomnej koordinácii činností.

⁸³ Zákon č. 165/2015 Z. z., Správny súdny poriadok v znení neskorších predpisov (ďalej len „**Správny súdny poriadok**“).

Tabuľka č.9 Komparatívny prehľad základných aspektov existujúcich regulačných sandboxov NBS a ÚRSO

	NBS	ÚRSO
Právny základ	• zriadenie a fungovanie sandboxu nie je špecificky legislatívne ukotvené v Zákone o dohľade⁸⁴, legislatívne odkazy sú najmä na ustanovenia o zverejňovaní informácií; • fungovanie sandboxu je komplexne upravené pravidlami vydanými NBS.	• zriadenie a fungovanie sandboxu nie je špecificky legislatívne ukotvené napr. v rámci Zákona o regulácii⁸⁵; • fungovanie sandboxu je čiastočne upravené osobitnou dokumentáciou súvisiacou s prihlasovaním sa do sandboxu (viď nižšie) a informáciami na stránke ÚRSO.⁸⁶
Základný cieľ	• uľahčiť implementáciu finančných inovácií na slovenskom finančnom trhu a pomôcť NBS lepšie porozumieť finančným inováciám; • napomôcť účastníkovi na základe konzultácií nastaviť finančnú inováciu v súlade s právnymi predpismi v pôsobnosti NBS a umožniť testovanie.	• podporiť inovácie, ktoré vedú k alebo majú potenciál viesť k zníženiu nákladov a konečnej ceny regulovaných komodít a služieb, zefektívňujú investície a prevádzku regulovaných subjektov a v konečnom dôsledku prinášajú nové produkty a služby pre spotrebiteľov v sieťových odvetviach; • získať informáciu o tom, ako implementovať nové projekty v existujúcom systéme (či regulačnom rámci) a ako ich potrebám prispôbiť predpisy a zákony.
Charakter sandboxu	Obmedzená pôsobnosť – sandbox sa sústreďuje na poskytovanie konzultácií zúčastneným subjektom, neupravuje výnimky z povoloňacieho procesu ⁸⁷ , a neupravuje spoluprácu s ostatnými orgánmi (s výnimkou cezhraničného testovania formou dohody s ostatnými orgánmi dohľadu iných členských štátov);	Obmedzená pôsobnosť – sandbox poskytuje viaceré možnosti podpory pre zúčastnené subjekty: (i) poradenstvo, (ii) formálna záštita ⁸⁸ , (iii) zníženie nákladov ⁸⁹ , neupravuje výnimky z povoloňacieho alebo dohľadového procesu ⁹⁰ a neupravuje spoluprácu s ostatnými orgánmi
Základné dokumenty	• pravidlá fungovania regulačného sandboxu, vrátane prihlášky a metodiky na posudzovanie kritérií⁹¹	• podmienky účasti v sandboxe⁹²; • prihláška do sandboxu⁹³.
Personálne kapacity pre	• 2 zamestnanci • V prípade výskytu ad hoc špecifickej potreby pri prevádzke sandboxu sú k	• 5 zamestnancov

⁸⁴ Zákon č. 747/2004 Z. z. o dohľade nad finančným trhom a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len "**Zákon o dohľade**").

⁸⁵ Zákon č. 250/2012 o regulácii v sieťových odvetviach v znení neskorších predpisov (ďalej len "**Zákon o regulácii**").

⁸⁶ <https://www.urso.gov.sk/regulacny-sandbox/>

⁸⁷ V prípade, že účastníkom je žiadateľ o povolenie na poskytovanie finančnej služby, musí tento účastník získať príslušné povolenie počas prípravnej fázy. Testovať finančnú inováciu v regulačnom sandboxe NBS môže až po tom, čo získa príslušné povolenie (licenčné konanie prebieha nezávisle od prípravnej fázy regulačného sandboxu). Testovanie finančnej inovácie nemá vplyv na povinnosti uložené účastníkovi osobitnými predpismi.

⁸⁸ Schválenie projektu poskytujúce stupeň formálnej záštity nad projektom má cieľ poskytnúť potrebné záruky voči ostatným orgánom štátnej správy, investorom a ďalším partnerom, že projekt nie je v konflikte s platnou legislatívou, ani Regulačnou politikou ÚRSO a jeho zámer je považovaný za prínosný z pohľadu ÚRSO.

⁸⁹ Premietnutie nákladov projektu schválených ÚRSO do oprávnených nákladov regulovaného subjektu počas doby trvania projektu. ÚRSO zároveň prihliada na možné dopady nákladov projektu na regulovanú cenu daného regulovaného subjektu.

⁹⁰ Projekt nemôže byť v rozpore s pravidlami a zásadami stanovenými legislatívou upravujúcou oblasť regulácie v sieťových odvetviach a nesmie poškodzovať práva, právom chránené záujmy a právne postavenie odberateľa.

⁹¹ Pravidlá fungovania regulačného sandboxu, dostupné na:

https://nbs.sk/_img/documents/_dohlad/fintech/sandbox/pravidla-sandbox-nbs.pdf

⁹² Podmienky účasti v regulačnom sandboxe, dostupné na:

https://www.urso.gov.sk/data/files/591_podmienky-ucasti-v-regsandboxe_1rocnik_2023-v4_final.pdf

⁹³ Žiadosť o účasť v schéme Regulačného sandbox, dostupné na:

https://www.urso.gov.sk/data/files/590_formular_ziadost-o-ucast-1rocnik_2023_v3_final.docx

	NBS	ÚRSO
prevádzku sandboxu⁹⁴	dispozícií aj personálne kapacity ostatných odborov NBS.	V prípade výskytu ad hoc špecifickej potreby pri prevádzke sandboxu sú k dispozícii aj personálne kapacity ostatných odborov ÚRSO.
Zúčastnené subjekty	- dohliadaný subjekt, - zahraničný dohliadaný subjekt, - žiadateľ o povolenie, - poskytovateľ služieb, - budúci dohliadaný subjekt, - NBS.	- akýkoľvek subjekt aktívny na trhu v sieťových odvetviach, napr.: akademické inštitúcie a orgány verejnej správy, regulované subjekty, iné podniky, vrátane malých a stredných firiem s inovatívnym produktom či službou, energetické spoločenstvá a tiež ďalší účastníci trhu;⁹⁵ - ÚRSO.
Počet zúčastnených subjektov/projektov	1 projekt (2 prepojení účastníci) v roku 2022 ⁹⁶	4 projekty v rámci nultého ročníka 2021
Fázy	- príhláška; - vyhodnotenie príhlášky - do 2 mesiacov odo dňa doručenia úplnej príhlášky; - prípravná fáza - konzultácie s NBS pre nastavenie finančnej inovácie v súlade s právnymi predpismi a stanovenie priebehu fázy testovania v podobe plánu testovania - trvá najviac 6 mesiacov; - fáza testovania - implementácia testovanej inovácie na trhu podľa plánu testovania max. 6 mesiacov; - ukončenie účasti - do 1 mesiaca po ukončení testovania účastník doručí do NBS záverečnú správu a do 1 mesiaca od doručenia záverečnej správy zorganizuje NBS záverečné stretnutie s účastníkom, aby spoločne prerokovali záverečnú správu a priebeh účasti v regulačnom sandboxe.	- príhláška; - vyhodnotenie príhlášky - do 3 mesiacov odo dňa doručenia úplnej príhlášky; - príprava projektu v spolupráci s ÚRSO; - schválenie projektu; - realizácia projektu – začiatok maximálne do 12 mesiacov - celková dĺžka trvania projektu max. 36 mesiacov (prvé priebežné výstupy projektu musia byť zverejnené 6 mesiacov od začatia aplikácie projektu v praxi); - výstupná správa s finálnymi výstupmi musí byť zverejnená do 12 mesiacov od ukončenia projektu; - trhové nasadenie otestovaného riešenia najneskôr do 2 rokov od úspešného ukončenia projektu; - kontrola vynaložených nákladov ako aj plnenia cieľov projektu priebežne na ročnej báze a po skončení projektu.
Časový rámec	cca. 16+ mesiacov	1-3 roky
Výsledok	záverečná správa zhrňujúca (i) priebeh testovania, (ii) posúdenie, či boli dosiahnuté očakávané výsledky testovania, (iii) problémy a neočakávané situácie, ktoré sa vyskytli počas testovania, a (iv) informáciu, či účastník plánuje pokračovať v ponúkaní finančnej inovácie klientom po ukončení svojej účasti v regulačnom sandboxe	- výstupná správa - možnosť uznania časti oprávnených ekonomických nákladov viažucich sa k regulovanej činnosti pri aplikácii do praxe - zohľadnenie výsledkov pri tvorbe legislatívy, či nastavení a presadzovaní pravidiel a postupov (vrátane regulačných odchýliek)

⁹⁴ Informácie poskytnuté zo strany NBS a ÚRSO (platné pre december 2023).

⁹⁵ Žiadateľom o projekt v rámci ÚRSO sandboxu musia byť minimálne dva subjekty a viac tvoriacich Skupinu žiadateľov podávajúcú spoločný projekt, pričom minimálne jedným zo subjektov je regulovaný subjekt na trhu sieťových odvetví v SR a druhým je výskumná inštitúcia alebo MSP pôsobiaci v oblasti aplikovaného výskumu a vývoja. Pri projektoch zameraných na ochranu zraniteľných odberateľov môže byť druhým subjektom aj mimovládna organizácia, alebo relevantný orgán štátnej správy alebo miestnej samosprávy.

⁹⁶ Viď Správa o činnosti inovačného hubu a regulačného sandboxu Národnej banky Slovenska 2022 dostupná na: <https://nbs.sk/dokument/d7e89f9b-bf63-4b80-857c-8b17614ba652/stiahnut?force=false>

Aktuálne nastavenie existujúcich regulačných sandboxov v SR sumarizované vyššie (a najmä sandboxu NBS, ktorého pravidlá sú regulované komplexnejšie, vrátane metodiky na posudzovanie kritérií na prístup do sandboxu) vo viacerých ohľadoch zohľadňuje základné požiadavky na sandboxy pre umelú inteligenciu predpokladané Nariadením ako napr. otvorený a transparentný prístup do sandboxu a zahrnutie možnosti účastníkov požadovať usmernenia s cieľom dosiahnuť súlad testovaného projektu/inovácie s právnymi predpismi v kompetencii príslušného regulátora.

Máme však za to, že požiadavky kladené Nariadením na zriadenie sandboxu pre umelú inteligenciu opodstatňujú komplexnejšie a robustnejšie riešenie najmä z pohľadu legislatívneho ukotvenia fungovania sandboxu pre umelú inteligenciu v podmienkach SR (kombináciou vyššie uvedených legislatívno-technických nástrojov, vrátane rámcovej zákonnej úpravy formou tzv. experimentálnej doložky a s konkrétnejšou reguláciou praktických aspektov formou vykonávacích regulačných aktov). To je odôvodnené najmä s prihliadnutím na: (i) požiadavky Nariadenia na zavedenie špecifických právomocí zriaďujúceho resp. iného príslušného orgánu (vrátane zmocnenia neprijíť žiadne administratívne donucovacie opatrenia za porušenie Nariadenia, ak potenciálni poskytovatelia zúčastnení na AI sandboxe plnia požiadavky Nariadenia), (ii) komplexnosť a prierezovosť fungovania AI sandboxu v prostredí prekrývajúcich sa kompetencií viacerých príslušných orgánov/regulátorov, a (iii) zabezpečenie súladu s vyššie uvedenými základnými regulačnými princípmi aplikujúcimi sa na zavádzanie sandboxov, vrátane princípov legality a právnej istoty.

Zároveň máme za to, že potreba zriadenia sandboxu pre umelú inteligenciu podľa Nariadenia predstavuje príležitosť pre zohľadnenie aj ďalších tzv. „best practices“ ohľadom fungovania sandboxov (nad rámec minimálnych požiadaviek Nariadenia) vyplývajúcich z benchmarkingu ďalších existujúcich sandboxov, ktoré sumarizujeme v časti 3.2.1 a 3.1.3.4 Štúdie nižšie. Naše odporúčania teda zohľadňujú tak vhodné prvky existujúcich sandboxov NBS/ÚRSO avšak ich dopĺňajú aj dodatočnými odporúčaniami z analýzy riešení v iných jurisdikciách v nasledovnej časti.

3.2 Analýza existujúcich experimentálnych regulačných prostredí (sandboxov) z 2 iných jurisdikcií, ktoré zaviedli regulačné opatrenia v oblasti AI

3.2.1 Prehľad riešení sandboxov pre systémy umelej inteligencie v Európe a vo svete

3.2.1.1 Španielsko

Španielsko, ako prvá krajina EÚ zareagovala na navrhovanú reguláciu systémov umelej inteligencie na základe Nariadenia, a vytvorila prvý sandbox pre testovanie systémov umelej inteligencie pod priamym dohľadom príslušných orgánov z pohľadu požiadaviek Nariadenia.⁹⁷

A. Ciele sandboxu

Sandbox je podporený Európskou komisiou a má slúžiť ako prostriedok na preskúmanie uskutočniteľnosti požiadaviek Nariadenia. Jeho cieľom je vytvoriť testovacie prostredie, v ktorom spoločnosti skúšajú vývoj a validáciu systémov AI, tak aby zabezpečili súlad s požiadavkami Nariadenia.⁹⁸

⁹⁷ Vid' napr. <https://www.pinsentmasons.com/out-law/news/spain-legislates-for-first-eu-ai-act-regulatory-sandbox>

⁹⁸ <https://digital-strategy.ec.europa.eu/en/news/first-regulatory-sandbox-artificial-intelligence-presented>

Očakáva sa, že zo sandboxu vzídu užitočné skúsenosti a osvedčené postupy pre implementáciu a monitorovanie požiadaviek zákona, ktoré budú slúžiť ďalším subjektom pri zosúlaďovaní ich systémov umelej inteligencie s požiadavkami regulácie AI, po tom, čo právne predpisy budú schválené a vstúpia do platnosti.⁹⁹

B. Princípy

Sandbox predpokladá spoluprácu medzi poskytovateľmi systémov AI a ich používateľmi. Účasť v sandboxe je podmienená splnením kritérií oprávnenosti (napr. stupeň inovácie, rizika a vyspelosti projektu, štátna príslušnosť), na ktorých dodržiavanie dohliada výbor odborníkov.¹⁰⁰ Predmetom testovania je vývoj a používanie i) vysoko rizikových systémov umelej inteligencie, ii) systémov umelej inteligencie na všeobecné účely a iii) základných modelov umelej inteligencie.¹⁰¹

Sandbox má vopred stanovenú dobu trvania. Jeho činnosť sa plánuje ukončiť 36 mesiacov po jeho spustení alebo po konečnom schválení Nariadenia.

C. Účastníci

Účastníci sandboxu sú vybraní na základe vyhlásenej výzvy, pričom ich prihlásenie a účasť v sandboxe je plne dobrovoľná. Počet účastníkov je limitovaný. Do sandboxu sú vybrané systémy umelej inteligencie, ktoré už pôsobia na trhu, ako aj systémy, ktoré v súčasnosti prechádzajú podstatnými zmenami, a systémy, ktoré síce na trhu ešte nie sú, ale dosiahli dostatočne pokročilú úroveň vývoja, aby mohli byť uvedené na trh alebo do prevádzky.

Zúčastniť sa môžu:

- **Dodávateľia** systémov umelej inteligencie, pričom za nich sa považuje každá súkromná právnická osoba, verejný orgán, subjekt verejného orgánu alebo subjekt akéhokoľvek iného druhu, ktorý vyvinul systém umelej inteligencie alebo pre ktorého ho vyvinula tretia strana, ak ho uvádza na trh alebo do prevádzky pod svojím vlastným alebo obchodným menom ako dodávateľ. Dodávateľia môžu mať jeden alebo viacero rôznych systémov; do sandboxu sa však môžu zapojiť len s jedným z týchto systémov.
- **Používatelia**, ktorí majú bydlisko alebo sú usadení v Španielsku, sú definovaní ako právnické osoby, verejné orgány alebo orgány verejného sektora, v rámci ktorých sa používa systém umelej inteligencie. Používatelia môžu mať prístup do sandboxu len vtedy, ak tak urobí aj príslušný dodávateľ.¹⁰²

D. Postup

Oprávnené subjekty sa do sandboxu registrujú prostredníctvom výzvy vyhlásenej príslušným ministerstvom na dobrovoľnej báze. Po uzavretí registrácie prebehne výberové konanie, ktoré overí kritériá oprávnenosti a určí finálne zloženie sandboxu, pričom sa uprednostňujú najinovatívnejšie, najkomplexnejšie, sociálne najvplyvnejšie a najvyzretejšie systémy AI.

⁹⁹ https://www.uria.com/documentos/circulares/1678/documento/13329/UM_ENG.pdf?id=13329&forceDownload=true

¹⁰⁰ <https://www.pinsentmasons.com/out-law/news/spain-legislates-for-first-eu-ai-act-regulatory-sandbox>

¹⁰¹ https://www.uria.com/documentos/circulares/1678/documento/13329/UM_ENG.pdf?id=13329&forceDownload=true

¹⁰² https://www.garrigues.com/en_GB/garrigues-digital/spain-artificial-intelligence-regulatory-sandbox-has-arrived

Účastníkom prijatým do sandboxu poskytne odborný poradný orgán, ktorý bude vytvorený špeciálne na tento účel, technické špecifikácie, predbežné usmernenia a individuálne poradenstvo o tom, ako splniť požiadavky a povinnosti Nariadenia. Následne sa pre každý systém AI určí plán implementácie týchto požiadaviek.

Keď účastník vypracuje plán činností potrebných na zabezpečenie toho, aby jeho systém splňal tieto požiadavky, je povinný predložiť vlastné posúdenie ich súladu.

Po vypracovaní hodnotiacej správy posúdi príslušný orgán sebahodnotenie každého účastníka. Potom buď navrhne zúčastnenému subjektu revidovať niektoré body svojho plánu, alebo potvrdí, že vyhlásenie o zhode je dostatočné (a bude vydaný záverečný akreditačný dokument).¹⁰³

E. Výhody

Sandbox uľahčí dodržiavanie požiadaviek a povinností stanovených Nariadením a umožní identifikovať prípadné ťažkosti alebo problémy, ktoré môžu vzniknúť v čase jeho uvedenia do praxe.

Podporí tiež výmenu informácií a skúseností medzi účastníkmi a verejnou správou vďaka čomu môžu byť navrhnuté zlepšenia predbežných usmernení a technických špecifikácií, čím sa predbežne prispeje k ich aktualizácii pred ich konečným uverejnením, ktoré sa sprístupní všetkým zainteresovaným stranám.

Okrem toho výsledky sandboxu budú zosumarizované a uverejnené v správe so závermi, ktorá prispeje k prebiehajúcim prácam na ďalšom formovaní Nariadenia.

3.2.1.2 Spojené kráľovstvo

Náročnosť orientácie v regulačných režimoch pre vývojárov podnietila v Spojenom kráľovstve vytvorenie sandboxu pre umelú inteligenciu. Toto prostredie bude prepájať regulačné orgány, aby priamo podporovali inovátorov a pomohli im dostať ich produkty na trh. Sandbox tiež umožní pochopiť, ako regulácia interaguje s novými technológiami a v prípade potreby túto interakciu pomôže vylepšiť. Pilotný sandbox pre AI plánuje vláda spustiť v priebehu roka 2024.¹⁰⁴

A. Ciele sandboxu

Cieľom sandboxu je podporiť nasadzovanie systémov umelej inteligencie a ich bezpečný vývoj. Taktiež sa snaží vytvoriť priestor na spoluprácu, v ktorom možno zdieľať poznatky a podporiť širšie pochopenie výziev a potenciálnych riešení. Súčasne sa usiluje odstrániť prekážky pre vývoj inovácií tým, že sa eliminuje zložitosť a právne riziká spojené s uvedením produktu na trh.

B. Princípy

Navrhovaný sandbox má za úlohu zaistiť, aby bola umelá inteligencia bezpečná a riadne regulovaná, avšak spôsobom, ktorý neobmedzuje inovácie a prístup k najnovším technológiám.

Za účelom vytvorenia efektívneho sandboxu sa do budúcnosti zvažovali 4 možnosti organizácie sandboxu:

¹⁰³ <https://www.lexology.com/library/detail.aspx?g=99939c25-d7bb-4d06-b154-4a972eb71e9b>

¹⁰⁴ <https://www.gov.uk/government/news/new-advisory-service-to-help-businesses-launch-ai-and-digital-innovations>

- **Jeden sektor, jeden regulátor:** Podpora inovátorov pri uvádzaní produktov AI na trh v spolupráci s jedným regulátorom a so zameraním len na jeden vybraný priemyselný sektor (napríklad zdravotníctvo).
- **Viacero sektorov, jeden regulátor:** Podpora inovátorov AI v spolupráci s jedným regulátorom, ktorý je schopný pracovať vo viacerých priemyselných odvetviach.
- **Jeden sektor, viacero regulátorov:** Vytvorenie sandboxu, ktorý funguje iba v jednom priemyselnom sektore, ale je schopný podporovať inovátorov AI, ktorých cesta na trh si vyžaduje interakciu s jedným alebo viacerými regulátormi pôsobiacimi v tomto sektore.
- **Viacero sektorov, viacero regulátorov:** Sandbox je schopný fungovať s jedným alebo viacerými regulátormi v jednom alebo viacerých priemyselných sektoroch, aby pomohol inovátorom AI dosiahnuť ich cieľový trh.

Fórum pre digitálnu reguláciu a spoluprácu - DRFC¹⁰⁵ (vládna agentúra zabezpečujúca väčšiu spoluprácu v rámci regulovania digitálnych záležitostí) bude nakoniec pilotovať štvrtú verziu (viacero sektorov, viacero regulátorov) a bude zodpovedné za spustenie a prevádzku tohto regulačného prostredia. Členovia DRFC pozostávajú z Úradu komisára pre informácie (Ofcom), Úradu pre hospodársku súťaž a trhy a Úradu pre finančné hospodárenie a sú známe ako "DRFC AI and Digital Hub".

Očakáva sa, že pilotný sandbox bude trvať približne rok a posúdi využitie priemyslu, uskutočniteľnosť služieb a spôsob interakcie s inovátormi. Inovátori a podniky, ktoré potrebujú poradenstvo, budú vyzvaní, aby sa do sandboxu prihlásili včasne. DRFC bude mať za úlohu poskytnúť inovačným subjektom podporu od regulačných orgánov v oblastiach, v ktorých ju potrebujú. Cieľom je zabezpečiť, že nové inovatívne technológie budú v súlade s prierezovými regulačnými režimami. Úspešní žiadatelia budú vybraní podľa kritérií, na ktorých sa spoločne dohodnú regulačné orgány a ministerstvo.

C. Účastníci

Sandbox je navrhnutý tak, aby bol priestorom spolupráce, ktorý spája odborné znalosti inovátorov, regulátorov, vlády i akademickej obce.

D. Postup

Ako prvé sa identifikujú prierezové regulačné problémy, ktoré majú dosah v reálnom svete a brzdia inovácie, a určia sa príležitosti na zlepšenie aktuálneho regulačného rámca. Ďalej sa poskytne poradenstvo podnikom, ktoré sa snažia orientovať v regulačnom prostredí a zmonitorujú sa vznikajúce trendy a príležitosti vo vývoji umelej inteligencie, aby sa zaistila efektívnosť regulačného rámca.

¹⁰⁵ <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum>

E. Výhody

Pilotovaný regulačný sandbox so sebou nesie množstvo výhod. Po prvé, podporuje inovácie: AI je rýchlo sa vyvíjajúca technológia a regulačné prostredie má problém držať krok. Sandbox umožňuje vývoj nových technológií AI v kontrolovanom prostredí, čím sa znižuje riziko porušenia zákonov alebo nariadení. Ukázalo sa, že to skracuje takzvaný „čas uvedenia na trh“ pre inovácie, čím sa novým podnikom poskytuje väčšia právna istota, čo vedie k väčšej inovácii. Súvisiacou výhodou je rýchlosť reakcie na nový technologický vývoj.

Sandbox je taktiež flexibilným a pohotovým nástrojom na reagovanie na nový vývoj a možno ho rýchlo upraviť, aby zohľadnil nové výzvy. Režim sandboxu zároveň poskytuje záruky ochrany spotrebiteľa. Systémy umelej inteligencie majú potenciál spôsobiť škody spotrebiteľom a regulačné sandboxy môžu pomôcť zabezpečiť, aby bolo používanie systémov umelej inteligencie bezpečné. Sandbox umožňuje testovať systémy AI v kontrolovanom prostredí, identifikovať a zmierniť potenciálne riziká. To môže pomôcť chrániť spotrebiteľov a zabezpečiť, aby mali dôveru vo vyvíjanú technológiu. Sandbox ďalej umožňuje spoluprácu - spája regulačné orgány, podniky a ďalšie zainteresované strany, aby spolupracovali na vývoji technológií AI. Táto spolupráca môže viesť k efektívnejším predpisom, ktoré vyvažujú potreby inovácií s verejnou bezpečnosťou. Tento proces učenia sa pre regulačné orgány je obojstranne výhodný a môže pomôcť vybudovať dôveru v technológiu a zvýšiť jej prijatie. Potenciálne nevýhody sú neadekvátne záruky, obmedzený rozsah, nepredvídané dôsledky a nedostatok konzistentnosti. Výzvou je taktiež, že štandardizácia AI, podobne ako sandboxy AI, a celý tento sektor sú v ranom štádiu vývoja. Ich vývoj teda bude prebiehať paralelne. V reakcii na to musia byť národné, regionálne a medzinárodné regulačné a štandardizačné rámce úzko koordinované.

3.2.2 Stručný prehľad existujúcich komerčných sandboxov a AI modelov z pohľadu technického zabezpečenia

Z pohľadu technického zabezpečenia prostredia existujú inovačné sandboxy, ktoré sú sprístupnené existujúcimi poskytovateľmi technológií AI napr. Azure AI Lab, Meta AI Sandbox, BigScience BLOOM, Google AI. Tieto (komerčné) sandboxy poskytujú prostredia pre vývoj, tréning a testovanie generatívnych modelov na základe princípov, pravidiel a zamerania jednotlivých poskytovateľov, pričom pri príprave štúdie a odporúčaní ohľadom fungovania AI sandboxu v prostredí Slovenskej republiky, boli zohľadnené ich prvky, ktoré sme považovali za prínosné v kontexte predmetu tejto štúdie.

Pre účely zodpovedného použitia systémov AI poskytovatelia deklarovali pravidlá alebo princípy zodpovedného použitia AI:

- **Azure AI Lab** je zameraný na testovanie súladu s princípmi, akými sú férovosť, bezpečnosť, spoľahlivosť, súkromie, inklúzia, transparentnosť zodpovednosť, avšak nie je primárne zameraný na overenie modelu s legislatívou.
- **Meta AI Sandbox** bol uvedený v máji 2023 a je určený pre digitálny marketing.
- **BigScience BLOOM** zavádza licencovanie pre zodpovednú umelú inteligenciu - Responsible AI License (RAIL), ktorej cieľom je prevencia nezodpovedného a škodlivého použitia systémov AI.
- **Google AI** formuluje praktiky pre zodpovedné AI, ktoré obsahujú všeobecné odporúčané praktiky pre umelú inteligenciu, férovosť, interpretovateľnosť, súkromie, ochrana a bezpečnosť.

Jednotlivé komerčné AI sandboxy majú vlastné definované princípy a pravidlá pre riešenia (Microsoft Responsible AI Standard, BigScience Ethical Charter, Google Responsible AI Practices), pričom posudzovanie v týchto sandboxoch nie je primárne zamerané na posudzovanie s Nariadením. Technologicky sú komerčné sandboxy postavené na proprietárnych technológiách a cloudovej infraštruktúre jednotlivých poskytovateľov.

Univerzita v Stanforde v roku 2023 posúdila základné AI modely s vtedajším návrhom Nariadenia, pričom oblasti hodnotenia súladu s Nariadením zoskupila podľa oblastí na:

- Dáta: dátové zdroje pre tréningovanie modelu, správa dát, autorské práva;
- Výpočty: výpočty a energia;
- Model: kapability a limitácie, riziká a mitigácie, evaluácia a testovanie;
- Nasadenie: strojovo-generovaný obsah, štáty, ktoré využívajú model, dokumentácia.

Uvedený spôsob vyhodnotenia môže byť jedným zo vzorov pri nastavovaní validačných a testovacích princípov predložených riešení v AI sandboxe, avšak je ho potrebné aktualizovať za účelom súladu s platným Nariadením ako aj prispôbiť tak, aby vyhovoval potrebám AI sandboxu v lokálnych podmienkach.

Pre ilustráciu uvádzame výsledok vyhodnotenia. Najvyššie možné skóre bolo určené 48, pričom BLOOM dosiahol: 36, OpenAI: 25, Google PaLM2: 27, Meta LLaMA: 21, ďalšie vyhodnotenie je zobrazené na Obrázku č. 1 nižšie.

Obrázok č.1.: Stanford Center for Research on Foundation Models - výstup posúdenia základných modelov EU Nariadenia

Grading Foundation Model Providers' Compliance with the Draft EU AI Act

Source: Stanford Center for Research on Foundation Models (CRFM), Institute for Human-Centered Artificial Intelligence (HAI)

	OpenAI	cohere	stability.ai	ANTHROPIC	Google	Hydrosphere	Meta	AI21 labs	ALPHA ALPHA	ELIUM EPR	
Draft AI Act Requirements	GPT-4	Cohere Command	Stable Diffusion v2	Claude 1	PaLM 2	BLOOM	LLaMA	Jurassic-2	Luminous	GPT-NeoX	Totals
Data sources	● ○ ○ ○	● ● ● ○	● ● ● ●	○ ○ ○ ○	● ● ● ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	22
Data governance	● ● ● ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	19
Copyrighted data	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	7
Compute	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ● ● ○	● ● ● ●	17
Energy	○ ○ ○ ○	● ● ● ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	● ● ● ●	16
Capabilities & limitations	● ● ● ●	● ● ● ○	● ● ● ●	○ ○ ○ ○	● ● ● ●	● ● ● ●	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	27
Risks & mitigations	● ● ● ●	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	16
Evaluations	● ● ● ●	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	● ● ● ○	15
Testing	● ● ● ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	10
Machine-generated content	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	● ● ● ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	● ● ● ○	21
Member states	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ●	○ ○ ○ ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	● ● ● ○	9
Downstream documentation	● ● ● ○	● ● ● ●	● ● ● ●	○ ○ ○ ○	● ● ● ●	● ● ● ●	● ● ● ○	○ ○ ○ ○	○ ○ ○ ○	● ● ● ○	24
Totals	25 / 48	23 / 48	22 / 48	7 / 48	27 / 48	36 / 48	21 / 48	8 / 48	5 / 48	29 / 48	

Singapurská agentúra IMDA (Infocomm Media Development Authority), ako národný regulátor pre telekomunikačné a poštové služby, zriadená singapurským Ministerstvom komunikácií a informácií vytvorila AI Sandbox v spolupráci so 16 komerčnými inštitúciami (vrátane Amazon, Google, IBM, Microsoft, Stability.AI a ďalších), ktorí vytvárajú spoločný základ pre porozumenie hodnotenia tzv. veľkých jazykových modelov (LLM) prostredníctvom evaluačného katalógu (Cataloguing LLM evaluations).

IMDA v spolupráci s AI Verify Foundation, ktorá má momentálne takmer 100 členov (<https://aiverifyfoundation.sg/foundation-members/>) vytvárajú testovací rámec a softvérové nástroje, ktoré budú vyhodnocovať AI systémy oproti medzinárodne uznávaným princípom, prostredníctvom štandardizovaných testov, ktoré budú konzistentné s AI regulačnými rámcami Európskej únie, OECD a Singapuru. (<https://aiverifyfoundation.sg/what-is-ai-verify>)

Na základe vyššie uvedeného prehľadu je možné predpokladať prispôbovanie komerčných ako aj mimoeurópskych AI sandboxov smerom k hodnoteniu súladu s pravidlami definovanými v Nariadení. Zároveň je však potrebné vytvorenie technologickej infraštruktúry AI sandboxu resp. sandboxov, ktoré budú posudzovať AI modely nezávislým posudzovaním založeným na pravidlách Nariadenia v rámci Európskej únie.

3.3 Odporúčania pre zriadenie sandboxu pre umelú inteligenciu v prostredí Slovenskej republiky

Táto časť Štúdie sumarizuje hlavné odporúčania ohľadom nastavenia sandboxu pre umelú inteligenciu v prostredí SR, ktoré vychádzajú zo zistení Štúdie uvedených v predchádzajúcich častiach, vrátane tzv. best practices vyplývajúcich z benchmarkingu existujúcich AI sandboxov v iných jurisdikciách.

3.3.1. Odporúčania reflektujúce základné legislatívne požiadavky Nariadenia

3.3.1.1 Potreba naplnenia základných požiadaviek legislatívy na AI sandboxy vyplývajúce z Nariadenia

Nastavenie sandboxu pre umelú inteligenciu v prostredí SR by malo zodpovedať základným požiadavkám na sandboxy (a s tým súvisiacim povinnostiam zriaďujúcich orgánov) vyplývajúcim z Nariadenia a delegovaných aktov, ktoré majú byť prijaté Komisiou v tomto ohľade (tieto základné požiadavky sú detailne rozpracované v časti 3.1.2.2 Štúdie vyššie) a zahŕňajú okrem iného:

- povinnosť (prípadne možnosť - viď vysvetlenia v časti 1.1.1 vyššie) zriadiť aspoň jeden sandbox pre umelú inteligenciu na vnútroštátnej úrovni, ktorý musí byť funkčný najneskôr v deň začatia uplatňovania Nariadenia,
- povinnosť nastaviť fungovanie AI sandboxu tak, aby prispel k naplneniu Nariadením stanovených cieľov,

- nastaviť fungovanie AI sandboxu tak, aby umožňovalo plnenie metodických, dohľadových, koordinačných a notifikačných povinností orgánu zriaďujúceho sandbox v zmysle Nariadenia v spolupráci s ostatných dotknutými OVM, a
- povinnosť zabezpečiť súlad so základnými princípmi fungovania AI sandboxu vyplývajúcimi z čl. 53 ods. 3 a ods. 4 Nariadenia a základnými modalitami pre fungovanie AI sandboxov v čl. 53a a 54a Nariadenia, ktoré sú zamerané na základné technicko-organizačné požiadavky a spoločne s pravidlami spracovania osobných údajov sú detailne rozpracované v rámci časti 3.2.1. (ii) tejto Štúdie.

3.3.1.2 Zriadenie sandboxu v gescii vnútroštátneho dozorného orgánu

Ako bolo uvedené vyššie v časti 3.1.3 s prihliadnutím na systematické a praktické aspekty (najmä pôsobnosť v oblasti vydávania usmernení a poradenstva týkajúceho sa vykonávania Nariadenia (čl. 59 ods. 7 Nariadenia) a dohľadu a kontroly v oblasti pôsobnosti Nariadenia (čl. 59 ods. 1 Nariadenia) odporúčame zvážiť zriadenie AI sandboxu v rámci pôsobnosti už existujúceho vnútroštátneho dozorného orgánu (OVM), ktorý bude určený SR v zmysle čl. 59 ods. 1 Nariadenia, a ktorý pre tieto účely bude môcť (čiastočne) využiť svoje existujúce kapacity, ak nebudú identifikované dôvody, pre ktoré by mal byť zriaďujúcim orgánom iný OVM SR.

Rovnako na tomto mieste opakujeme, že pre účely tejto Štúdie (a v zmysle výsledkov stretnutia MIRRI/PwC dňa 22.11.2023) vychádzame z predpokladu, že s prihliadnutím na organizačno-technické, nákladové hľadiská, ako aj legislatívno-technické hľadiská, v oblasti AI dôjde v prvej fáze k zriadeniu jedného experimentálneho regulačného prostredia v rámci SR, na ktorého činnosti však budú participovať aj ďalšie OVM v rozsahu ich (najmä metodických a dohľadových) právomocí v príslušných oblastiach, ktoré sa budú týkať systémov AI posudzovaných v rámci sandboxu v súlade s princípom jeden regulátor (resp. jeden sandbox) - viacero sektorov.

3.3.1.3 Legislatívno-technická forma úpravy zriadenia AI sandboxu

Pre zriadenie sandboxu navrhujeme zvážiť využitie kombinácie postupov uvedených v časti 3.2.2. Štúdie vyššie, a to najmä zakotvenie právneho rámca pre fungovanie sandboxu formou zákonnej doložky o experimentálnom režime s konkrétnejšou reguláciou praktických aspektov fungovania AI sandboxu (najmä pravidiel prihlasovania, hodnotenia kritérií a pod.) formou iných vykonávacích regulačných aktov príslušných orgánov (najmä zriaďujúceho orgánu (OVM) - vid' tiež časť 2.1.1) umožňujúcich väčšiu flexibilitu reagovania na prípadné zmeny alebo požiadavky súvisiace s fungovaním AI sandboxu. Pri formulácii príslušných predpisov navrhujeme prihliadať na minimálne štandardy definované v časti 3.2.2 Štúdie. Spolupráca ostatných OVM môže byť zabezpečená kombináciou zákonných a zmluvných nástrojov (napr. dohody v zmysle Kompetenčného zákona).

3.3.2 Odporúčania reflektujúce existujúcu prax v oblasti regulačných sandboxov

3.3.2.1 Kapacitné plánovanie

Z dôvodu zabezpečenia riadnej a efektívnej prevádzky je potrebné prijať adekvátne kapacitné obmedzenia, ktoré budú reflektovať personálne, organizačné, časové a technologické možnosti zriaďovateľa (zriaďujúceho orgánu). Z tohto dôvodu odporúčame umožnenie účasti v sandboxe len takým systémom umelej inteligencie, ktoré už pôsobia na trhu, alebo v súčasnosti prechádzajú podstatnými zmenami, prípadne, ktoré síce na trhu ešte nie sú, ale dosiahli dostatočne pokročilú úroveň vývoja, aby mohli byť uvedené na trh alebo do prevádzky. V súvislosti s kapacitným plánovaním je možné zvážiť aj riadenie kapacity AI sandboxu prostredníctvom nastavenie testovania v rámci kapacitne obmedzených a/alebo periodicky sa opakujúcich sa kôl, pričom podrobnosti je možné upraviť v pravidlách sandboxu.

3.3.2.2 Vypracovanie metodických a podporných dokumentov

Zabezpečenie hladkého a bezproblémového priebehu procesu zriadenia a fungovania sandboxu pre umelú inteligenciu si vyžaduje vydanie príslušných aktov a dokumentov v kompetencii zriaďujúceho orgánu (s odporúčaným zmocnením na základe zákonnej experimentačnej doložky), ktoré budú detailne upravovať fungovanie sandboxu, štandardizovať príslušné procesy a zároveň inštruovať zúčastnených aktérov pri ich realizácii. K základným dokumentom by mali patriť:

- **Plán sandboxu:** dokument obsahujúci náležitosti stanovené pre plán sandboxu v zmysle delegovaných aktov Komisie (ak budú takéto akty vydané), ktorý môže obsahovať všeobecný rámec pre fungovanie sandboxu, definovanie cieľov, nastavenie trvania sandboxu (prípadne jeho jednotlivých kôl), základné náležitosti plánu testovania medzi zriaďovateľom a účastníkom AI sandboxu a pod.;
- **Pravidlá fungovania sandboxu:** Dokument, ktorý bude v potrebnom detaile objasňovať kompletný proces, podmienky a kritéria vstupu a povinnosti jednotlivých účastníkov sandboxu. Dokument umožní predovšetkým budúcim uchádzačom získať lepšiu predstavu o fungovaní sandboxu, čo im pomôže v ich rozhodovaní o možnosti zapojiť sa a tiež zvýši mieru pripravenosti na účasť.
- **Metodika na posudzovanie kritérií na vstup do sandboxu:** Dokument, ktorý by štandardizoval vyhodnocovanie žiadostí na vstup do sandboxu pri zohľadnení požiadaviek Nariadenia a cieľov definovaných zriaďujúcim orgánom. Metodika by mala obsahovať jasné kritéria pre vyhodnotenie:
 - pripravenosti žiadateľa na účasť v sandboxe,
 - existencie potreby testovania,
 - vecnej opodstatnenosti navrhovaného riešenia (potvrdenie, že ide o AI technológiu),
 - prioritizácie projektov s prihliadnutím na definované priority voči MSP, podporu sociálne a environmentálne prospešných výsledkov,
 - splnenia podmienky pozitívneho dopadu.
- Prihláška do sandboxu
- Písomný záznam o aktivitách vykonaných v rámci sandboxu.

- Hodnotiaca/záverečná správa.
- Výročné správy o fungovaní sandboxu (v zmysle čl. čl. 53 ods. 5b Nariadenia).
- Akákoľvek iná dokumentácia, ktorej vyhotovenie bude požadované Komisiou v rámci delegovaných aktov týkajúcich sa prevádzky AI sandboxov.

3.3.2.3 Jeden regulátor (jeden sandbox) - viacero sektorov

V Spojenom Kráľovstve sa rozhodli pilotovať regulačný sandbox pre umelú inteligenciu v podobe - viacero sektorov, viacero regulátorov, kedy sandbox funguje s jedným alebo viacerými regulátormi v jednom alebo viacerých priemyselných sektoroch. Tento prístup je náročný z kapacitného, organizačného, odborného či finančného hľadiska, a preto je vhodnejší v prostredí, kde už existujú zavedené a overené postupy a potrebné know-how. V podmienkach slovenského technologického sektora z toho dôvodu odporúčame zvážiť prístup - "jeden regulátor (jeden sandbox), viacero sektorov", kedy v rámci implementovaného sandboxu pre umelú inteligenciu funguje jeden primárny regulátor - zriaďovateľ sandboxu spolupracujúci podľa potreby s ostatnými OVM, pričom sandbox bude pokrývať riešenia AI vo viacerých priemyselných odvetviach.

3.3.2.4 Pilotný režim sandboxu

Účelom pilotného režimu AI sandboxu je prostredníctvom testovania prijatého technologického riešenia identifikovať chyby, nedostatky alebo prípadný nesúlad so stanovenými požiadavkami buď pred uvedením sandboxu do plnej prevádzky alebo v rámci prvého kola jeho prevádzky resp. v rámci preddefinovaného počiatočného obdobia. Zriaďujúci orgán tak môže posúdiť jeho účinnosť a použiteľnosť a tiež minimalizovať riziko chýb a množstvo prípadných dodatočných investícií. Spustenie pilotného programu zároveň umožňuje zhromaždiť spätnú väzbu od účastníkov, regulačných orgánov a ďalších zainteresovaných strán, ktoré môžu poskytnúť cenné informácie na vylepšenie a prispôsobenie sandboxu pre AI. Aj vo vzťahu k zriadeniu AI sandboxu v prostredí SR odporúčame nastaviť úvodné fázy fungovania AI sandboxu v rámci pilotného režimu.

3.3.2.5 Vytvorenie databázy záujemcov o účasť v sandboxe

Zámerom vytvorenia sandboxu je tiež prepojenie záujmu slovenských dohliadaných subjektov so záujmom technologických firiem pôsobiacich na trhu. Odporúčame preto vytvoriť databázu záujemcov o spoluprácu, kde môžu tieto subjekty a firmy prejsť dopyt po spolupráci. To pomôže regulačným orgánom pochopiť potreby a záujmy rôznych účastníkov trhu v oblasti umelej inteligencie a technológií. Táto databáza by umožnila sledovať, kto má záujem o účasť a aký typ technológií sa snažia rozvíjať alebo implementovať.

3.3.2.6 Poistenie poskytovateľov ako možná podmienka účasti

Potenciálni poskytovatelia majú byť zodpovední za akúkoľvek škodu spôsobenú tretím stranám v dôsledku experimentov, ktoré sa v sandboxe uskutočňujú. V prípadoch, kedy sú inovácie v AI spojené s rizikami, ktoré by mohli mať výrazný negatívny vplyv na zákazníkov, údaje alebo iné subjekty, odporúčame zvážiť zaradenie poistenia poskytovateľa za škodu medzi požadované bezpečnostné opatrenia alebo podmienky účasti (v závislosti od možnosti dostupnosti komerčného poistenia na trhu).

3.3.2.7 Flexibilita a adaptabilita sandboxu

Umelá inteligencia má mnoho aplikácií a použití vo virtuálnom aj fyzickom svete. Flexibilný sandbox dokáže zohľadniť rozmanitosť týchto aplikácií a ich špecifické potreby. Zároveň sa mení legislatívne prostredie a výzvy týkajúce sa etiky, bezpečnosti a zodpovednosti, čo si bude vyžadovať testovanie nových prístupov a metód. Odporúča sa preto pri tvorbe sandboxu prijať také riešenie, ktoré umožní rýchlu reakciu na tieto zmeny a prispôsobenie sa novým požiadavkám a normám (vrátane flexibilnej regulácie fungovania sandboxu prostredníctvom vykonávacích regulačných aktov, promptným zohľadňovaním spätnej väzby od zúčastnených subjektov a sledovaním zahraničných best practices).

3.3.2.8 Periodické hodnotenie fungovania AI sandboxu

Odporúčame, aby bol zavedený systém na periodické vyhodnocovanie fungovania celého sandboxu (napr. po uzavretí príslušného kola), a to najmä za nasledovnými účelmi:

- **Zlepšenie riadenia a organizácie sandboxu:** Na základe zhodnotenia priebehu implementácie jednotlivých projektov je možné identifikovať oblasti, ktoré potrebujú zlepšenie [tak na individuálnej báze ako aj vo vzťahu k celkovému fungovaniu sandboxu. To môže zahŕňať úpravu pravidiel, podmienok účasti, zlepšenie podpory pre účastníkov alebo ďalšie opatrenia na zvýšenie účinnosti a úspešnosti sandboxu.
- **Zabezpečenie transparentnosti a zodpovednosti:** Zriaďujúci orgán zabezpečí verejnú prezentáciu výsledkov hodnotenia [vrátane prípravy výročných správ¹⁰⁶, ktorá pomáha udržiavať dôveru a transparentnosť voči zainteresovaným stranám a verejnosti.
- **Podpora ďalšieho rozvoja:** Na základe výsledkov hodnotenia je možné vypracovať odporúčania a návrhy na ďalší rozvoj a zdokonalenie sandboxu. Tieto informácie môžu byť využité ako základ pre vylepšenie a optimalizáciu procesov, aby sandbox mohol účinnejšie podporovať inovácie v oblasti AI a zároveň chrániť záujmy a bezpečnosť zúčastnených strán.
- **Celkové vyhodnotenie fungovania sandboxu:** Hodnotenie, vrátane vypracovania záverečnej správy, by malo nastať aj po ukončení fungovania sandboxu buď na základe rozhodnutia zriaďujúceho orgánu alebo po uplynutí doby na ktorú bol sandbox zriadený, ak bude zriadený na určité obdobie.

3.3.2.9 Technická podpora pre sandbox

Odporúčame zvážiť, ktoré z potrebných personálnych kapacít (uvedených v časti 4.3 Štúdie) budú zabezpečené interne príslušným určeným vnútroštátnym dozorným orgánom/orgánom zriaďujúcim sandbox, zdieľanými kapacitami s inými OVM, alebo prípadne externými kapacitami.

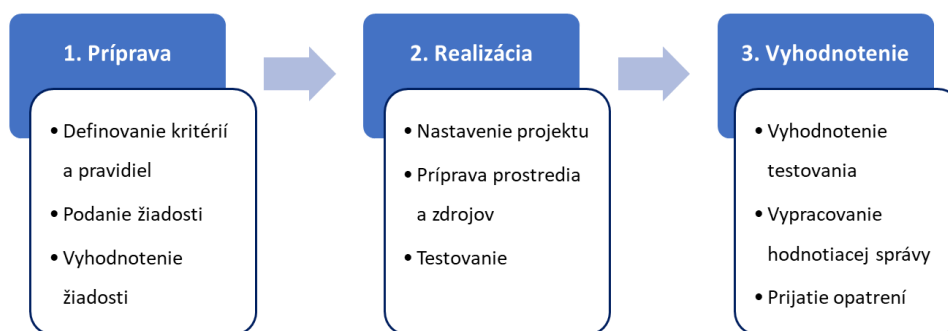
Odporúčame tiež zvážiť technickú podporu procesov v rámci sandboxu pre umelú inteligenciu, pomocou vhodného softvérového vybavenia a riešenia pre správu žiadostí a súvisiacich pracovných tokov, evidenciu uchádzačov, zúčastnených strán, testovania ako aj podporu ochrany a správy údajov, ktoré bližšie analyzujeme ďalej v tejto Štúdii.

¹⁰⁶ Článok 53 ods. 5b Nariadenie

3.3.3 Odporúčaný priebeh projektu v sandboxe pre umelú inteligenciu v SR

V tejto časti Štúdie sumarizujeme odporúčaný priebeh posudzovania prihláseného AI riešenia realizovaného v rámci sandboxu pre umelú inteligenciu prostredníctvom popisu jeho troch (navrhovaných) hlavných fáz a odporúčaných aktivít. Fáza, ktorá samotného vytvorenia a nastavenia legislatívneho a inštitucionálneho rámca fungovania sandboxu pre umelú inteligenciu v zmysle Nariadenia, popisujeme v rámci odporúčaní v časti 3.3.1 Štúdie. Dôležitou súčasťou sú tiež technicko-organizačné aspekty zabezpečenia sandboxu, ktoré sú podrobne analyzované v častiach 4.3, 5.1 a 5.2 tejto Štúdie.

Obrázok č.2.: Fázy realizácie projektu posudzovania systému AI v sandboxe pre umelú inteligenciu v zmysle Nariadenia



3.3.3.1 Príprava na účasť v AI sandboxe

Prvým krokom, ktorý je potrebný vykonať pred samotným spustením posudzovania projektov AI v rámci sandboxu je stanovenie podmienok účasti vo vzťahu k subjektom pôsobiacim na trhu, ktoré predstavujú budúcich potenciálnych účastníkov sandboxu. V súvislosti s prípravou samotného spustenia sandboxu bude zriaďujúci orgán zodpovedať za:

- **Definovanie kritérií účasti:** Zriaďujúci orgán je zodpovedný za stanovenie kritérií, ktoré musia subjekty spĺňať pre vstup do sandboxu. Tieto kritériá budú definovať rozsah projektov AI, ktoré sú vhodné na testovanie a ďalšie podmienky ako veľkosť podniku, účel testovania, ochrana údajov či transparentnosť algoritmov ako aj ďalšie kritériá v súlade so základnými regulačnými princípmi fungovania sandboxu.
- **Formulácia pravidiel a podmienok:** Zriaďujúci orgán musí vytvoriť pravidlá a podmienky, ktoré musia účastníci dodržiavať počas testovacieho obdobia. Tieto pravidlá môžu obsahovať požiadavky na správu rizík, bezpečnosť údajov a zodpovednosť za výsledky testovania AI technológie.
- **Vytvorenie žiadosti o účasť:** Zriaďujúci orgán vytvorí vzor formálnej žiadosti, ktorú subjekty musia predložiť pre účasť v sandboxe. Táto žiadosť by mala obsahovať podrobnosti o projekte, plnení preddefinovaných kritérií pre účasť v sandboxe, cieľoch testovania, technických špecifikáciách, opatreniach na riadenie rizík a ďalšie náležitosti definované zriaďujúcim orgánom.

Následne žiadatelia určeným spôsobom predkladajú žiadosti o účasť v sandboxe. Zriaďujúci orgán je zodpovedný aj za proces hodnotenia a schvaľovania predložených žiadostí o účasť. Tento proces zahŕňa posúdenie žiadostí na základe stanovených kritérií a rozhodovanie o tom, ktoré projekty budú určené na testovanie v rámci sandboxu. Zriaďovateľ sandboxu umožní žiadateľovi vstúpiť do AI sandboxu, ak splní príslušné preddefinované kritériá, a to najmä:

- žiadateľ spĺňa definované podmienky na osobné postavenie účastníka;
- predmetom účasti je aktivita resp. AI systém, ktorá spadá do definovaného okruhu pôsobnosti sandboxu;
- žiadateľ preukáže preddefinovanú úroveň schopnosti splniť požiadavky stanovené zriaďujúcim orgánom a technickú pripravenosť na testovanie;
- žiadateľ identifikuje riziká a nastavenie opatrení na ich zmiernenie;
- je preukázaná potreba testovania - účasť v regulačnom sandboxe prispeje k úspešnej implementácii AI inovatívneho riešenia na slovenskom trhu;
- žiadateľ preukáže, že inovácia je nová, alebo málo uplatňovaná na slovenskom trhu;
- riešenie má pozitívne dopady na zákazníkov na slovenskom trhu, prípadne na ďalšie ciele definované zriaďujúcim orgánom (napr. podpora MSP, podpora sociálne a environmentálne prospešných výsledkov).

3.3.3.2 Realizácia - posudzovanie AI riešenia v AI sandboxe

Po schválení žiadosti sa nastaví spôsob posudzovania AI riešenia (vrátane jeho testovania) v rámci sandboxu. Zriaďujúci orgán a žiadateľ sa stretnú a vzájomne komunikujú, aby presne definovali a objasnili očakávania, požiadavky a procesy, ktoré budú súčasťou testovacieho obdobia. Výsledkom prípravy je:

- **Presné stanovenie cieľov:** Diskusia o konkrétnych cieľoch, ktoré má projekt dosiahnuť počas testovacieho obdobia v sandboxe. To môže zahŕňať merateľné ukazovatele úspešnosti, ktoré sa majú dosiahnuť.
- **Určenie rozsahu testovania:** Definícia rozsahu a oblastí, v ktorých bude projekt testovaný. Taktiež sa môžu špecifikovať podmienky, za ktorých bude testovanie prebiehať.
- **Plánovanie a harmonogram:** Diskusia o pláne a harmonograme testovania, čo zahŕňa stanovenie termínov, fáz testovania, monitorovanie pokroku a zhodnotenie výsledkov.
- **Identifikácia rizík a opatrení:** Zhodnotenie potenciálnych rizík spojených s testovaním a stanovenie opatrení na ich riadenie a minimalizáciu.
- **Úprava vzťahov:** Po dohode na podmienkach a pláne testovania sa odporúča záväzne upraviť vzájomné vzťahy medzi žiadateľom a zriaďujúcim orgánom (napr. prostredníctvom akceptácie záväzných pravidiel), vrátane úpravy detailov o testovacom období, právach a povinnostiach oboch strán, ochrane údajov, rozsahu testovania, či podmienkach ukončenia testovania.
- **Príprava prostredia a zdrojov:** Žiadateľ by mal začať prípravou prostredia a zdrojov potrebných na testovanie riešenia. To môže zahŕňať prípravu technických prostriedkov, úpravu systémov, prípravu dát a ďalšie potrebné kroky.

Tento prvý kontakt a prípravná fáza sú dôležité pre úspešnú implementáciu testovania a následné záverečné hodnotenie. Pomáha zúčastneným stranám presne pochopiť očakávania, ciele a procesy, čo prispieva k hladkému priebehu testovacieho obdobia a zabezpečuje, že všetky strany majú jasnú predstavu o svojich úlohách a zodpovednostiach. Zároveň je dôležité udržiavať otvorenú komunikáciu medzi žiadateľom a zriaďujúcim orgánom (ako aj ostatnými zúčastnenými OVM a ďalšími subjektmi) počas celej tejto fázy. Zdieľanie informácií, riešenie otázok a rýchle reagovanie na prípadné problémy je kľúčové pre úspešnú realizáciu testovania.

Po schválení plánu účastník implementuje svoje inovatívne AI riešenie a začína jeho testovanie v kontrolovanom prostredí sandboxu. Dané riešenie alebo aplikácia umelej inteligencie sa v kontrolovanom prostredí testuje a overuje voči stanoveným regulačným a bezpečnostným kritériám a pravidlám. V tomto prostredí sa môže umožniť subjektom testovať svoje AI riešenia (v povolenom a právny predpismi predpokladanom rozsahu) bez niektorých obmedzení alebo regulácií, ktoré by inak platili mimo tohto špecifického rámca. Cieľom je skúmať schopnosti, efektívnosť a možné riziká daného AI systému pri reálnom použití alebo aplikácii.

Počas testovania v AI sandboxe sa zhromažďujú údaje, monitorujú sa výsledky a riešia sa prípadné problémy. Tento proces umožňuje subjektom identifikovať a riešiť nedostatky, zlepšovať riešenia a zároveň umožňuje zriaďujúcemu orgánu (a ďalším OVM) a zúčastneným stranám získať dôveru a lepšie pochopenie, ako sa dané AI riešenia správajú v skutočných podmienkach. Testovanie v sandboxe pomáha identifikovať a minimalizovať riziká spojené s používaním AI technológií a zároveň podporuje inovácie v tomto sektore pri zachovaní dôležitého bezpečnostného a regulačného rámca.

Zriaďujúci orgán má počas testovania príslušného AI riešenia niekoľko dôležitých úloh:

- **Dozor a monitorovanie:** Zriaďujúci orgán sleduje a monitoruje priebeh testovania príslušného AI riešenia v sandboxe. Jeho úlohou je dohliadať na to, aby účastníci dodržiavali stanovené pravidlá a podmienky ako aj príslušné právne predpisy, pričom v rámci tohto procesu spolupracuje aj s ostatnými OVM v príslušnom rozsahu.
- **Hodnotenie rizík:** Zriaďujúci orgán sa zaoberá hodnotením rizík, ktoré môžu byť spojené s testovaným AI riešením. Snaží sa identifikovať potenciálne nebezpečenstvá alebo nesprávne použitie technológie a navrhuje opatrenia na ich minimalizáciu.
- **Poskytovanie poradenstva a usmernení:** Zriaďujúci orgán môže (v prípade potreby v spolupráci s ostatnými príslušnými sektorovými orgánmi dohľadu) poskytnúť účastníkovi sandboxu poradenstvo a usmernenia, ako sa vyhnúť rizikám a dodržiavať pravidlá a predpisy počas testovacieho obdobia.
- **Zhromažďovanie údajov a správa výsledkov:** Zriaďujúci orgán zbiera relevantné dáta a informácie o výsledkoch testovania. Tieto údaje sú potrebné na vyhodnotenie účinnosti a bezpečnosti testovaného riešenia a na prípravu relevantných výstupov (správy, záznamy z posudzovania).
- **Zabezpečenie transparentnosti a správy rizík:** Zriaďujúci orgán by mal zabezpečiť transparentnosť celého procesu účasti v sandboxe a viesť evidenciu o rizikách, výsledkoch a iných dôležitých aspektoch spojených s testovaním.

Účastník sa podieľa na testovaní predovšetkým plnením nasledujúcich úloh:

- **Implementácia riešenia:** Účastník by mal implementovať svoje AI riešenie podľa podmienok a pravidiel stanovených a/alebo dohodnutých so zriaďujúcim orgánom.
- **Testovanie a validácia:** Po implementácii sa AI riešenie testuje a validuje v kontrolovanom prostredí sandboxu a/alebo v reálnom prostredí za podmienok dohodnutých so zriaďujúcim orgánom. Účastník by mal uskutočňovať testy, ktoré overia funkčnosť, účinnosť a presnosť AI riešenia.
- **Hodnotenie rizík a monitorovanie:** Účastník by mal pravidelne hodnotiť riziká spojené s používaním svojho AI riešenia a monitorovať jeho správanie a fungovanie počas testovacieho obdobia v zmysle príslušných podmienok.
- **Súlad a dodržiavanie podmienok:** Je dôležité, aby účastník dodržiaval stanovené pravidlá a podmienky. To zahŕňa dodržiavanie právnych predpisov, podmienky účasti v sandboxe stanovené zriaďujúcim orgánom, vrátane (prípadných) zmluvne dohodnutých podmienok, pravidiel na správu údajov, ochranu súkromia, transparentnosť a ďalšie požiadavky, ktoré boli stanovené počas fázy prípravy.
- **Poskytovanie spätnej väzby a informácií:** Účastník je povinný poskytovať zriaďujúcemu orgánu sandboxu pravidelnú spätnú väzbu o výsledkoch testovania, problémoch, ktoré sa vyskytli a akékoľvek ďalšie informácie dôležité pre záverečné hodnotenie.
- **Spolupráca s OVM:** Ak sa počas testovania vyskytnú problémy alebo riziká, účastník je povinný o nich informovať stanoveným spôsobom, pričom by mal úzko spolupracovať so zriaďujúcim orgánom, ako aj s ďalšími zúčastnenými OVM na identifikácii a riešení týchto otázok.

3.3.3.3 Vyhodnotenie posudzovaného projektu

Zriaďujúci orgán a účastník vyhodnocujú výsledky testovania. Zisťujú úspechy, nedostatky a prípadné riziká spojené s používaním AI riešenia počas testovacieho obdobia. Na základe testovania sa vypracuje správa o výsledkoch testovania, ktorý zahŕňa podrobnosti o tom, ako AI riešenie fungovalo, identifikujú sa silné a slabé miesta a predovšetkým sa formulujú odporúčania na odstránenie zistených nedostatkov. Zriaďujúci orgán preskúma výsledky testovania a analyzuje správu o testovaní, pričom pri vyhodnocovaní môže komunikovať s príslušnými OVM. Týmto spôsobom sa rozhodne, či AI riešenie spĺňa stanovené ciele, pravidlá a normy sandboxu a najmä, či je v súlade s požiadavkami Nariadenia. Na základe výsledkov posudzovania/testovania môže dôjsť k pozitívnemu rozhodnutiu, ďalším úpravám alebo testovaniu, alebo ku zastaveniu projektu v prípade závažných nedostatkov či nezhôd s právnymi normami.

Dôležitou súčasťou ukončenia procesu posudzovania a testovania konkrétneho projektu je hodnotenie priebehu realizácie prostredníctvom spätnej väzby zo strany všetkých zúčastnených strán. Toto hodnotenie slúži na:

- **Posúdenie dosiahnutých výsledkov projektu:** Zriaďujúci orgán zhodnotí, do akej miery sa dosiahli stanovené ciele a očakávania v priebehu implementácie. To zahŕňa posúdenie úspechov, ako napríklad dosiahnutie zhody s požiadavkami Nariadenia, ich prínos pre inovácie, alebo riešenia identifikovaných problémov.

- **Identifikácia výziev a obmedzení projektu:** Hodnotenie umožňuje identifikovať a pochopiť prípadné problémy, výzvy alebo obmedzenia, ktoré mohli ovplyvniť priebeh implementácie. Tieto informácie sú kľúčové pre neustále zlepšovanie fungovania a efektívnosti tak konkrétnych projektov ako aj sandboxu ako takého.

4 Analýza náročnosti implementácie experimentálneho regulačného prostredia (sandboxu) v prostredí SR

4.1 Vyhodnotenie náročnosti vytvorenia a prevádzky experimentálneho regulačného prostredia podľa požiadaviek pripravovanej európskej legislatívy a relevantných osvedčených postupov.

V nasledovných častiach Štúdie uvádzame rámcové zhodnotenie náročnosti implementácie experimentálneho regulačného prostredia (sandboxu) v prostredí SR pri zohľadnení právno, technicko-organizačných a iných relevantných hľadísk.

4.2 Zhodnotenie aktuálneho regulačného prostredia vo vzťahu k zriadeniu sandboxu pre umelú inteligenciu v prostredí SR a identifikácia materiálnych právno-legislatívnych rizík na zohľadnenie vo vzťahu k zriaďovaniu sandboxu pre umelú inteligenciu

4.2.1 Stručné zhodnotenie aktuálneho regulačného prostredia a potreby očakávanej legislatívnej a regulačnej predprípravy fungovania sandboxov v slovenskom právnom prostredí

Ako už bolo uvedené v časti 3.2 Štúdie (*Analýza právneho rámca pre implementáciu sandboxov v zmysle požiadaviek Nariadenia a legislatívy SR*) vyššie, v súčasnosti v právnom prostredí Slovenskej republiky neexistuje komplexná legislatívna úprava pôsobnosti regulačných sandboxov (vo vzťahu k systémom umelej inteligencie alebo iným riešeniam), a to či už vo vzťahu k úprave právneho základu zriaďovania sandboxov a/alebo stanovenia konkrétnych požiadaviek na ich fungovanie. Ako vyplýva z porovnania aktuálneho režimu fungovania existujúcich sandboxov NBS a ÚRSO (viď časť 3.1.3.4 Štúdie vyššie), tieto sandboxy nevychádzajú z jednotného legislatívneho základu a líšia sa tak čo sa týka formy aj obsahu. Rovnako ani Nariadenie aktuálne neupravuje konkrétny postup ani formu, ktorou má byť sandbox (resp. sandboxy) pre umelú inteligenciu (v zmysle požiadaviek Nariadenia) v prostredí konkrétneho členského štátu EÚ zriadený.

S prihliadnutím na uvedené teda Slovenská republika (i) má značnú voľnosť akým spôsobom ciele a požiadavky Nariadenia vo vzťahu k zriadeniu a fungovaniu sandboxu naplní (pri rešpektovaní požiadaviek na fungovanie sandboxu stanovených Nariadením) a (ii) môže si vybrať najvhodnejší spôsob zohľadňujúci okrem iného preferovanú štruktúru inštitucionálneho rámca pre aplikáciu Nariadenia (viď aj časť 2.1 Štúdie vyššie).

Z analýzy existujúceho právneho rámca máme tiež za to, že v súčasnosti neexistujú materiálne legislatívne prekážky pre zriadenie a fungovanie sandboxu predpokladaného Nariadením. To potvrdzuje aj aktuálne pôsobenie regulačných sandboxov NBS a ÚRSO v právnom prostredí Slovenskej republiky.

Na druhej strane konkrétne špecifiká pre zriadenie a fungovanie sandboxu a výber najvhodnejšieho riešenia budú závisieť aj od toho akým spôsobom budú implementované požiadavky Nariadenia najmä vo vzťahu k inštitucionálnemu rámcu predpokladanému Nariadením do existujúceho legislatívneho a inštitucionálneho rámca Slovenskej republiky (najmä čo sa týka určenia príslušného vnútroštátneho dozorného orgánu a orgánu zriaďujúceho AI sandbox a nastavenia spolupráce s ostatnými OVM), a to okrem iného po zohľadnení záverov a odporúčaní TSI Analýzy.

S prihliadnutím na požiadavky Nariadenia (bez ohľadu na problematiku sandboxov), a to najmä, no bez obmedzenia, požiadavky na zavedenie špecifických právomocí vnútroštátneho dozorného orgánu predpokladaných Nariadením, bude pre ich implementáciu v slovenskom právnom prostredí potrebná komplexná legislatívna úprava formou vydania nového zákona a/alebo novelizácie aktuálnych zákonov (okrem iného po zohľadnení záverov a odporúčaní TSI Analýzy v relevantnom rozsahu), v rámci ktorej bude možnosť zavedenia základnej úpravy fungovania AI sandboxu aj na zákonnej úrovni.

V tomto ohľade máme tiež za to, že požiadavky kladené Nariadením na zriadenie sandboxu pre umelú inteligenciu opodstatňujú komplexnejšie a robustnejšie riešenie (v porovnaní s existujúcimi regulačnými sandboxmi NBS a ÚRSO) najmä z pohľadu legislatívneho ukotvenia fungovania sandboxu pre umelú inteligenciu v podmienkach SR. Pre zriadenie sandboxu pre účely umelej inteligencie v prostredí SR teda navrhujeme zvážiť kombináciu legislatívno-technických nástrojov uvedených v časti 3.1.3.1 Štúdie, vrátane rámcovej zákonnej úpravy sandboxu formou tzv. experimentálnej doložky a s konkrétnejšou reguláciou praktických aspektov fungovania sandboxu (najmä pravidiel prihlasovania, hodnotenia kritérií a pod.) formou iných vykonávacích regulačných aktov príslušného orgánu (resp. orgánov) umožňujúcich vyššiu flexibilitu reagovania na prípadné zmeny alebo požiadavky súvisiace s fungovaním sandboxu.

To je odôvodnené najmä s prihliadnutím na: (i) požiadavky Nariadenia na zavedenie špecifických právomocí zriaďujúceho resp. iného príslušného orgánu (vrátane zmocnenia neprijíť žiadne administratívne donucovacie opatrenia za porušenie Nariadenia, ak potenciálni poskytovatelia zúčastnení na sandboxe plnia požiadavky Nariadenia), (ii) komplexnosť a prierezovosť fungovania sandboxu v prostredí prekrývajúcich sa kompetencií viacerých príslušných orgánov/regulátorov, a (iii) zabezpečenie súladu so základnými regulačnými princípmi aplikujúcimi sa na zavádzanie sandboxov, vrátane princípov legality a právnej istoty (viď tiež časť 3.1.3.2 Štúdie vyššie).

Zároveň máme za to, že potreba zriadenia sandboxu pre umelú inteligenciu podľa Nariadenia predstavuje príležitosť pre zohľadnenie aj ďalších tzv. „best practices“ ohľadom fungovania sandboxov (nad rámec minimálnych požiadaviek Nariadenia) vyplývajúcich z benchmarkingu ďalších existujúcich sandboxov, ktoré sumarizujeme v časti 3.2.1 a 3.1.3.4 Štúdie vyššie.

Hlavné riziká súvisiace s potrebou komplexnej legislatívnej úpravy a legislatívno-technickým nastavením sandboxu pre umelú inteligenciu v prostredí SR, ako aj možnosti ich mitigácie, sú sumarizované v časti 4.6. Štúdie (tabuľka č. 10 nižšie), ktorá sumarizuje prehľad materiálnych rizík na zohľadnenie vo vzťahu k zriaďovaniu sandboxu pre umelú inteligenciu z pohľadu oblastí, ktoré boli predmetom Štúdie.

4.3 Analýza požadovaného organizačného zabezpečenia potrebného pre fungovanie experimentálneho regulačného prostredia.

4.3.1 Návrh základného organizačného zabezpečenia fungovania sandboxu pre umelú inteligenciu v SR

V tejto časti analyzujeme požadované organizačné zabezpečenie fungovania regulačného sandboxu. Uvádzame očakávané personálne kapacity potrebné na fungovanie sandboxu pre umelú inteligenciu v zmysle Nariadenia v prostredí Slovenskej republiky:

- **Vedúci sandboxu:** Nominovaná osoba by mala v súvislosti s organizáciou sandboxu pôsobiť v pozícií projektového a finančného manažéra. K hlavným úlohám a zodpovednostiam patrí riadenie podporného tímu a koordinácia a dohliadanie na všetky relevantné súčasti fungovania sandboxu. Zabezpečuje, (i) že všetky procesy a postupy sú zosúladené a dodržiavané v súlade s príslušnými predpismi a regulačnými štandardmi, (ii) komunikáciu so všetkými zúčastnenými stranami (vrátane ostatných zúčastnených OVM) a (iii) vedie tímové stretnutia. Z finančného hľadiska má na starosti sledovanie finančných aspektov sandboxu a zodpovedať tak za správu rozpočtu, vypracovanie finančných správ a sledovanie projektových nákladov.
- **Odborník na reguláciu:** Osoba s právnickým vzdelaním a s odbornými znalosťami v oblasti právnych a regulačných rámcov týkajúcimi sa umelej inteligencie (vrátane Nariadenia), ochrany osobných a iných údajov, bezpečnostných predpisov a iných predpisov súvisiacich s prevádzkou sandboxu. Odborník na reguláciu (i) sa zaoberá právnymi aspektmi regulácie AI projektov v rámci sandboxu, vrátane etických otázok, (ii) vykonáva analýzy právnych predpisov, (iii) zabezpečuje právnu podporu fungovania sandboxu, (iv) monitoruje splnenie požiadaviek Nariadenia a iných relevantných predpisov, (v) pomáha pri tvorbe regulačných opatrení vo vzťahu k projektom v sandboxe a (vi) zabezpečuje komunikáciu a spoluprácu s ostatnými zúčastnenými OVM v rámci svojich kompetencií.
- **Špecialista na umelú inteligenciu a technológie:** Odborník s hlbokými znalosťami systémov umelej inteligencie, strojového učenia a súvisiacich technológií, ktorý dokáže hodnotiť a usmerňovať projekty súvisiace s umelou inteligenciou.

Jeho úlohou je v spolupráci s ostatnými pracovníkmi sandboxu a ostatných zúčastnených OVM poskytovať technickú podporu a poradenstvo pri hodnotení AI projektov v rámci sandboxu v zmysle splnenia požiadaviek Nariadenia a iných relevantných predpisov. Taktiež sa podieľa na vytváraní technických noriem a usmernení pre fungovanie sandboxu.

- **Podporný personál:** Súčasťou podporného personálu v rámci sandboxu by mali byť osoby, ktoré budú zabezpečovať administratívnu a technickú podporu pre každodenné prevádzkovanie, logistiku a dokumentáciu sandboxu. Z hľadiska technickej podpory je potrebné, aby zodpovedná osoba zabezpečila správu databáz a informačného systému potrebného pre **efektívne** fungovanie sandboxu a vykonávaných procesov. Podporný personál sa tiež stará o komunikáciu s verejnosťou, tvorbu komunikačných stratégií, spravuje webové stránky, sociálne médiá a organizuje podujatia, aby informoval verejnosť o dianí v sandboxe.

Odporúčame zvážiť, ktoré z uvedených personálnych kapacít budú zabezpečené interne zriaďujúcim orgánom (t.j. osobami, ktoré budú zabezpečovať prevádzku sandboxu v rámci ich primárnej pracovnej náplne), zdieľanými kapacitami zriaďujúceho orgánu (t.j. osobami, ktoré sa budú podieľať na fungovaní sandboxu popri ich primárnej funkcii v rámci zriaďujúceho orgánu), alebo prípadne externými kapacitami.

Odhadované interné kapacity pre fungovanie regulačného sandboxu:

	Odhadované dedikované kapacity na fungovanie regulačného sandboxu – prípravná a implementačná fáza	Odhadované dedikované kapacity na prevádzku regulačného sandboxu
Vedúci sandboxu	1	1
Odborník na reguláciu	1	2
Špecialista na umelú inteligenciu a technológie	1	2
Podporný personál – Projektový manažér	1	1
Podporný personál – Administratívny pracovník	1	2
Spolu	5	8

Poznámka: Kapacity sú odhadované pri predpokladanom spracovaní a posudzovaní 20-tich prihlášok ročne.

4.3.2 Možnosti zriadenia doplnkových organizačných štruktúr v rámci sandboxu pre umelú inteligenciu

Nad rámec možného základného organizačného vymedzenia sandboxu pre umelú inteligenciu definovaného v časti 4.3.1 vyššie je, pre (i) podporu fungovania, (ii) vyššiu flexibilitu a (iii) možnosť zapojenia aj ostatných relevantných aktérov v rámci ekosystému umelej inteligencie¹⁰⁷ do AI sandboxu, možné zvážiť aj kreovanie rôznych stálych alebo *ad hoc* hodnotiacich a/alebo poradných štruktúr (najmä komisie/výbory, pracovné skupiny), ktoré budú pôsobiť v rámci organizačnej štruktúry AI sandboxu. Tieto môžu byť tvorené internými kapacitami zriaďujúceho orgánu ako aj externými kapacitami (napr. z prostredia ekosystému AI v SR, zamestnancami iných OVM SR participujúcich na prevádzke AI sandboxu (v tomto kontexte vid' najmä Tabuľku č. 2 (Prehľad relevantných OVM SR a ostatných zainteresovaných osôb vo vzťahu k zriadeniu sandboxu predpokladaného Nariadením v podmienkach SR)).

Tieto štruktúry môžu byť zapojené do všetkých fáz kreovania a fungovania AI sandboxu v želanom rozsahu, vrátane (i) zapojenia sa do konzultácií pri definovaní základných parametrov sandboxu (napr. kritériá pre vstup, hodnotenie) v legislatívno-prípravnej fáze, (ii) participácie na prevádzke AI sandboxu (zapojenie zástupcov do hodnotiacich/kontrolných orgánov najmä posudzovanie žiadostí o vstup do

¹⁰⁷ Vid' najmä čl. 53a ods. 2 písm. d) Nariadenia a časť 2.1.1.1 Štúdie. Napr. zástupcovia MSP, startupov, akademickej obce, občianskej spoločnosti a pod. (vid' Tabuľka č. 2 vyššie).

AI sandboxu, hodnotenie projektov/riešení, poradenstvo pri *ad hoc* otázkach), a (iii) hodnotenia celkovej funkčnosti AI sandboxu a definovania podnetov na zefektívnenie jeho fungovania.

Konkrétna štruktúra, zodpovednosti a spôsob fungovania týchto orgánov (vrátane stanovenia spôsobu rozhodovania, odmeny za účasť v orgánoch) môžu byť flexibilne stanovené príslušnými aktmi zriaďujúceho orgánu (napr. v rámci interných organizačných aktov, štatútov a pod.) s prihliadnutím na finálne nastavenie zariadenia AI sandboxu a preferencie zriaďujúceho orgánu.

4.4 Stanovenie alternatív podoby implementácie sandboxu pre umelú inteligenciu v zmysle Nariadenia a výber odporúčaného budúceho riešenia.

Vo vzťahu k legislatívno-technickým a inštitucionálnym alternatívam implementácie sandboxu pre umelú inteligenciu (v zmysle Nariadenia v prostredí SR) vid' naše závery a odporúčania v častiach 3.3.1 a 4.2.1 Štúdie vyššie. Na tomto mieste je možné v danom ohľade poukázať najmä na odporúčanie zväziť zriadenie jedného AI sandboxu v rámci pôsobnosti už existujúceho OVM, ktorý bude určený SR v zmysle čl. 59 ods. 1 Nariadenia ako vnútroštátny dozorný orgán, a ktorý pre tieto účely využije svoje existujúce kapacity, ak nebudú identifikované dôvody, pre ktoré by mal byť zriaďujúcim orgánom iný OVM SR, a to najmä s prihliadnutím na systematické a praktické aspekty (najmä pôsobnosť v oblasti vydávania usmernení a poradenstva týkajúceho sa vykonávania Nariadenia (čl. 59 ods. 7 Nariadenia) a dohľadu a kontroly v oblasti pôsobnosti Nariadenia (Čl. 59 ods. 1 Nariadenia).

4.5 Identifikácia technického riešenia na základe analýzy požiadaviek.

Spôsob identifikácie technického riešenia vychádza predovšetkým z požiadaviek definovaných v predošlých častiach tejto Štúdie. Pre podporu vykonávania funkcií AI sandboxu je možné využiť tak bežné kancelárske aplikácie a balíky (textový editor, tabuľkový procesor a pod.) ako aj softvérové nástroje podporujúce automatizované spracovanie procesov s funkciami správy údajov.

Z hľadiska používateľskej prívetivosti, konzistentnosti postupov, flexibilnej nastaviteľnosti a ochrany údajov je perspektívnym riešením využitie kolaboračných nástrojov. Tieto nástroje podporujú interakciu rôznych skupín používateľov, umožňujú vytváranie oddelených "pracovných zón", podporu bezpečného prístupu k údajom, verzionovanie testovacích scenárov a výsledkov ako aj zaznamenávanie výstupov kontroly a validácie.

Prístup k návrhu technického riešenia je preto zameraný najmä na identifikáciu biznis služieb a procesov, funkcií, aplikačných modulov, ktoré v čo najširšej miere podporujú identifikované požiadavky a funkcie AI sandboxu (zohľadňujúc najmä požiadavky Nariadenia). Popis návrhu riešenia je uvedený v časti 5 tejto Štúdie.

Ďalšie odporúčané kroky pre identifikáciu technického riešenia, ktoré nie sú predmetom tejto Štúdie avšak do budúcnosti je ich potrebné zväziť sú: (i) podrobná funkčná a technická špecifikácia požiadaviek - zohľadňujúca aj požiadavky ostatných účastníkov; a (ii) návrh postupov, procesov, metodík a vzorovej dokumentácie (žiadosť, testovacie scenáre vyjadrenie a pod.) pre realizáciu funkcií AI sandboxu.

4.6 Detekcia základných rizík a prekážok, ktoré môžu zabrániť alebo skomplikovať implementáciu sandboxu pre umelú inteligenciu v zmysle Nariadenia v prostredí SR

V tabuľke uvedenej nižšie uvádzame základný sumár materiálnych právno-legislatívnych rizík na zohľadnenie vo vzťahu k zriaďovaniu sandboxu pre umelú inteligenciu v zmysle Nariadenia a možné spôsoby mitigácie identifikovaných rizík.

Tabuľka č.10. Sumár materiálnych právno-legislatívnych rizík na zohľadnenie

Riziko	Spôsob mitigácie
V rámci finalizácie textu Nariadenia môže dôjsť k určitým úpravám textu s vplyvom na niektoré aspekty zriaďovania AI sandboxov (nad rámec/rozdielne v porovnaní s predpokladmi Štúdie), vrátane zmeny rozsahu povinností a kompetencií vnútroštátnych orgánov, zapojenia iných OVM SR a/alebo úpravy modalít fungovania AI sandboxov.	Aktívne sledovanie a participácia na legislatívnych procesov na úrovni Komisie pri zapojení MIRRI a ďalších relevantných OVM a promptné reagovanie na špecifikáciu požiadaviek.
Nebude prijatá národná legislatíva predpokladaná v súvislosti s potrebou implementovať požiadavky Nariadenia, vrátane určenia OVM zodpovedného za dohľad/zriadenie sandboxu (a/alebo zavádzajúca príslušnú doložku o experimentálnom režime) alebo jej kvalita nebude zodpovedať požiadavkám Nariadenia a odporúčaniam vyplývajúcim zo Štúdie.	Aktívne zapojenie MIRRI a ostatných relevantných OVM do legislatívneho procesu so zohľadnením odporúčaní vyplývajúcich zo Štúdie a TSI Analýzy (v relevantnom rozsahu).
Nebude včas implementovaný inštitucionálny rámec predpokladaný Nariadením vrátane určenia OVM zodpovedného za dohľad/zriadenie AI sandboxu a/alebo nebude implementovaný korektne, vrátane jasného rozdelenia pôsobnosti príslušných OVM.	Aktívne zapojenie MIRRI a ostatných relevantných OVM do legislatívneho procesu so zohľadnením odporúčaní vyplývajúcich zo Štúdie a TSI Analýzy (v relevantnom rozsahu). Jasná úprava právomocí OVM v legislatívnom procese a prípadne v dohodách o spolupráci pri zriaďovaní/fungovaní AI sandboxu v zmysle Kompetenčného zákona.
Neexistencia alebo oneskorené vydanie delegovaných predpisov Komisie týkajúcich sa prevádzkovania AI sandboxu v zmysle čl. 53a Nariadenia, s rizikom potreby neskoršej úpravy parametrov sandboxu pre účely zabezpečenia súladu s danými požiadavkami Komisie.	Aktívne sledovanie a participácia na legislatívnych procesov na úrovni Komisie pri zapojení MIRRI a ďalších relevantných OVM a promptné reagovanie na špecifikáciu požiadaviek. V prípade, že špecifikácia nebude vydaná v príslušnom čase - nastavenie AI sandboxu v zmysle základných požiadaviek vyplývajúcich z Nariadenia a best practices vyplývajúcich zo Štúdie a následná úprava parametrov AI sandboxu podľa potreby.
Nepodarí sa prijať interné akty orgánu zriaďujúceho AI sandbox regulujúce konkrétnosti fungovania AI sandboxu a/alebo ich kvalita bude nedostatočná.	Aktívna komunikácia a/alebo participácia na procese prípravy AI sandboxu zo strany určeného zriaďujúceho orgánu a iných OVM, vrátane procesov ohľadom legislatívno-technického ukotvenia AI sandboxu so zohľadnením odporúčaní vyplývajúcich zo Štúdie.
Partnerské OVM nebudú pripravené na zapojenie sa do prevádzky AI sandboxu v zmysle Nariadenia a/alebo implementačnej legislatívy.	Aktívne zapojenie MIRRI a ostatných relevantných OVM do legislatívneho procesu so zohľadnením odporúčaní vyplývajúcich zo Štúdie a TSI Analýzy (v relevantnom rozsahu). Komunikáciu o nastavení fungovania AI sandboxu a participácii jednotlivých OVM začať v dostatočnom predstihu.
Nejasný zodpovednostný režim súvisiaci s prevádzkovaním AI sandboxu.	Vhodná legislatívna úprava reflektujúca požiadavky vo vzťahu k zodpovednostnému režimu Nariadenia, vrátane čl. 53. ods. 4 Nariadenia ¹⁰⁸ a/alebo príslušná úprava v rámci konkrétnych pravidiel AI sandboxu (napr. vrátane zavedenia požiadavky na potrebu dojednania poistenia zodpovednosti za škodu pre účastníkov sandboxu).

¹⁰⁸ V tomto kontexte upozorňujeme na zjavne nesprávny preklad čl. 53. ods. 4 v slovenskom znení pozmeňujúcich návrhov Európskeho parlamentu Nariadenia naznačujúceho zodpovednosť zriaďovateľa sandboxu, pričom v anglickom aj českom znení je zodpovednosť za škodu spôsobenú tretím stranám v dôsledku experimentov, ktoré sa v AI sandboxe uskutočňujú jasne alokovaná na účastníka/poskytovateľa AI sandboxu.

Identifikované riziká technickej implementácie riešenia sandboxu pre umelú inteligenciu nižšie predstavujú základný prehľad najvýznamnejších rizík, ktoré môžu vzniknúť pri projekte (t.j. príprave alebo implementácii) alebo prevádzke technologického riešenia pre podporu sandboxu v praxi.

Tabuľka č.11 Sumár základných rizík a prekážok technickej implementácie riešenia

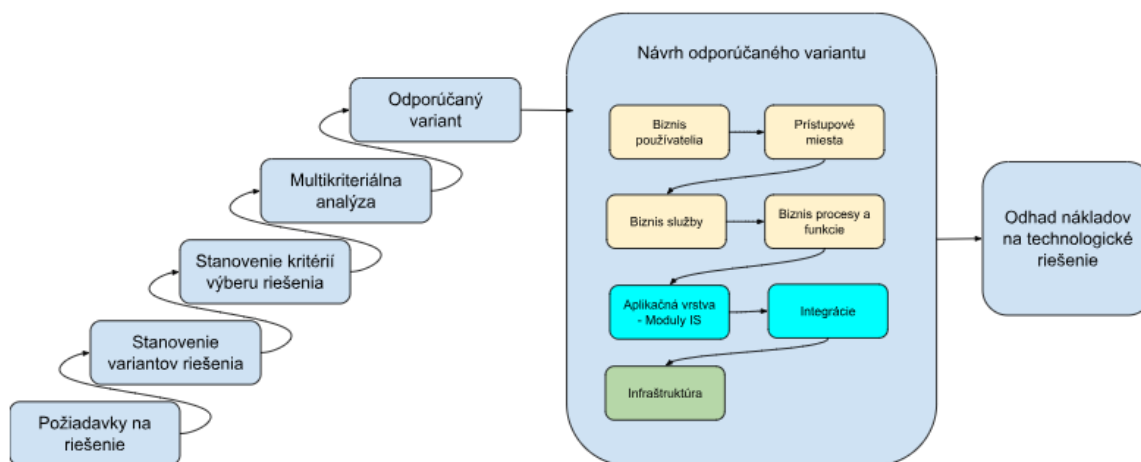
Riziko	Spôsob mitigácie
Častá zmena pravidiel, procesov alebo bezpečnosti pre podporu AI sandboxu. Neustále meniace sa pravidlá môžu skomplikovať nastavenie technického prostredia a oddialiť jeho využitie.	Využitie flexibilnej platformy pre implementáciu riešenia AI sandboxu môže zjednodušiť prispôbovanie procesov hodnotenia v budúcnosti, ako aj flexibilné zapojenie rôznych účastníkov
Dlhá doba obstarania technického riešenia. Zdlhavé odsúhlasenie zadania pre obstaranie zákazky na strane zadávateľa môže spôsobiť oneskorenie v začiatku používania riešenia.	Nastavenie plánu obstarávania, zdrojov a prioritizácie u zadávateľa riešenia (zriaďujúceho orgánu).
Dlhá doba dodania riešenia do prevádzky zo strany dodávateľa môže spôsobiť oneskorenie v začiatku používania riešenia.	Nastavenie jasného plánu, míľnikov pri obstarávaní pre dodanie diela, stanovenie kritérií pre výber skúseného dodávateľa, identifikácia rizík a zabezpečenie skúseného projektového riadenia za obe strany.
Nevyvážené využitie technického riešenia - nedostatočné alebo naopak preťaženie technického riešenia pre podporu AI sandboxu môže spôsobiť - pri nevyužití: investované prostriedky nebudú účelne použité v plánovanom čase, pri preťažení: kapacitný problém a tým aj oneskorenie v hodnotení a celkovej prevádzke sandboxu.	Nastavenie procesu prioritizácie skúsenými hodnotiteľmi v rámci spoločnej kolaboračnej platformy. Nastavenie plánu hodnotení a ich automatizácia (notifikácie, monitorovanie, reportovanie a pod.) Nastavenie optimálnych lehôt pre plynulé využitie procesných kapacít. Nastavenie správnej kapacity dátových úložísk pre využitie technickej kapacity testovania a archivácie.

5 Analýza identifikovaného technického riešenia

5.1 Návrh technického riešenia z pohľadu dizajnu, infraštruktúry a funkčných požiadaviek na sandbox pre umelú inteligenciu v zmysle Nariadenia

Tento návrh je založený na základných legislatívnych požiadavkách pre sandboxy (experimentálne regulačné prostredia) pre umelú inteligenciu s cieľom overenia súladu inovačných systémov umelej inteligencie s požiadavkami Nariadenia. Na základe záverov uvedených vo vyššie uvedených častiach Štúdie (najmä časti 3.3.1 a 4.2.1) je návrh riešenia koncipovaný pre zriaďujúci orgán, ktorý bude určený v rámci existujúceho OVM (viď časť 4.4 vyššie).

Obrázok č.3: Postup pri stanovení variantu technického riešenia sandboxu z pohľadu aplikačnej a technologickej vrstvy



V zmysle požiadaviek Nariadenia, sandbox pre umelú inteligenciu *“musí poskytovať kontrolované prostredie, ktoré na obmedzený čas pred uvedením inovačných systémov umelej inteligencie na trh alebo do prevádzky podľa konkrétneho plánu uľahčuje ich vývoj, testovanie a validáciu.”*

Okrem požiadaviek definovaných v nasledujúcej tabuľke (ktoré bude potrebné aktualizovať podľa potreby s prihliadnutím na dodatočné špecifikácie, ktoré môžu byť definované Komisiou v rámci prijatia delegovaných aktov predpokladaných čl. 53a Nariadenia, bude systém pre podporu AI sandboxu musieť obsahovať funkcionality na validáciu splnenia všetkých ďalších požiadaviek Nariadenia (a akýchkoľvek ďalších aplikovateľných predpisov), vrátane povinností v zmysle článku 16 Nariadenia na príslušné systémy umelej inteligencie, ktoré však nie sú v súčasnej dobe publikované

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie ¹⁰⁹ zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
1.	Základná funkcionálna - umožnenie vstupu do AI sandboxu pre fyzické aj virtuálne produkty	AI sandbox musí byť implementovaný tak, aby umožnil vývoj, testovanie a validáciu systémov AI, ktoré sa môžu používať samostatne ako softvérový systém, integrované (vstavaním) do fyzického výrobku, na napomáhanie funkčnosti fyzického výrobku bez toho, aby doň boli integrované (nevstavané), alebo sa majú používať ako súčasť umelej inteligencie väčšieho systému	Odôvodnenie (6b) a (71)	Podávanie žiadosti o posúdenie s Nariadením ¹¹⁰	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie
2.	Základná funkcionálna - umožnenie sledovania celého procesu fungovania AI sandboxu (workflow) od podania žiadosti (prípadne štádia predbežného vyjadrenia záujmu o účasť/konzultácií), výberu, účasti a opustenia AI sandboxu, vrátane sledovania plynutia príslušných lehôt.	Postupy, procesy a administratívne požiadavky na podávanie žiadostí, výber, účasť a odchod zo AI sandboxu musia byť jednoduché, ľahko zrozumiteľné, jasne komunikované a v súlade s harmonizovanými požiadavkami stanovenými Komisiou. Zriaďujúce orgány musia informovať žiadateľov o svojom rozhodnutí do 3 mesiacov od podania žiadosti o prístup do AI sandboxu. Účasť na AI sandboxe musí byť obmedzená na obdobie, ktoré je primerané zložitosti a rozsahu projektu;	Článok 53a ods. 2	Podávanie žiadosti o posúdenie s Nariadením Zobrazenie podaných žiadostí, monitorovanie stavu a údajov Notifikovanie a zasielanie správ	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie

¹⁰⁹ V znení, ktoré je reflektované v rámci Štúdie (viď vyššie) - to sa aplikuje aj vo vzťahu k nasledovným sekciám Štúdie.

¹¹⁰ Ak sa v rámci tejto tabuľky používa výraz "posudzovanie zhody", znamená posudzovanie zhody s požiadavkami Nariadenia, ak z textu alebo kontextu nevyplýva inak.

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
3.	Základná funkcionálna - podpora hodnotenia rizikivosti AI systému vstupujúceho do AI sandboxu v zmysle kritérií stanovených Nariadením najmä podpora identifikácie vysokorizikových systémov, na ktoré sa vzťahujú špecifické komplexné požiadavky Nariadenia a podpora identifikácie sektorových predpisov aplikovateľných na vstupujúci AI systém]	AI sandbox musí byť implementovaný tak, aby umožnil rýchlu a ľahkú identifikáciu vysokorizikových systémov, na ktoré sa vzťahujú komplexnejšie požiadavky Nariadenia ako aj identifikáciu ďalších relevantných sektorových predpisov a požiadaviek, ktoré bude potrebné zohľadňovať pri testovaní príslušných AI systémov. V tomto ohľade vid' napr. čl. 40 Nariadenia v zmysle ktorého vysokorizikové systémy umelej inteligencie a základné modely, ktoré sú v zhode s harmonizovanými normami EÚ alebo ich časťami, sa považujú za systémy, ktoré sú v zhode s požiadavkami stanovenými v príslušných ustanoveniach Nariadenia, pokiaľ sa uvedené normy na tieto požiadavky vzťahujú.	Odôvodnenie (27) Hlava III Článok 40 a nasl.	Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul konfigurácie testovania, validácie a evidencií
4.	Základná funkcionálna - uľahčenie/čiastočná automatizácia kontroly splnenia kritérií oprávnenosti a výberu, prípadne	Proces vstupu do AI sandboxu musí podporovať možnosť účasti každého, kto spĺňa kritériá oprávnenosti a výberu a umožniť široký a rovnaký prístup.	Článok 53a ods. 2 písm. a) a b)	Registrowanie uchádzača alebo účastníka	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
	splnenia kritérií MSP/(sociálnej/environmentálnej) prospešnosti projektov a následná archivácia záznamov					
5.	Základná funkcionálna - umožnenie komunikácie s OVM/orgánmi dohľadu/inými stakeholdermi zapojenými do prevádzky AI sandboxu, zdieľania výstupov pre paralelné/následné procesy posudzovania zhody/dohľadu a včasné notifikácie v prípade identifikovaných rizík	Nastavenie AI sandboxu musí podporovať zapojenie príslušných orgánov dohľadu do dohľadu nad jeho aspektmi v rozsahu ich príslušných úloh a právomocí, a zdieľanie výstupov zo AI sandboxu pre účely postupov posudzovania zhody alebo kontrol v rámci dohľadu nad trhom.	Článok 53a ods. 1g, 2 a 3	Posudzovanie zhody s Nariadením - komunikácia Notifikovanie a zasielanie správ	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
6.	Základná funkcionality - umožnenie kontroly platenia poplatkov pre neoslobodené subjekty	Prístup k AI sandboxu musí byť nastavený ako bezplatný len pre MSP a startupy bez toho, aby boli dotknuté mimoriadne náklady, ktoré môžu vzniknúť zriaďujúcemu orgánu. V prípade iných subjektov je možné aktuálne uvažovať o príslušnej forme spoplatnenia.	Článok 53a ods. 2 písm. c)	Registrowanie uchádzača alebo účastníka	Riadenie regulačného procesu	Kolaboračný modul Portál a používateľské rozhranie
7.	Základná funkcionality - zahrnutie komunikačného kanálu v rámci prostredia AI sandboxu na komunikáciu s účastníkmi	Za účelom podpory výskumu a vývoja riešení AI, ktoré podporujú sociálne a environmentálne prospešné výsledky je v prípade potreby možné v rámci AI sandboxu vytvoriť dostupný vyhradený kanál, na komunikáciu s projektmi s cieľom poskytovať usmernenia a odpovedať na otázky týkajúce sa vykonávania Nariadenia.	Článok 54a ods. 2 písm. c)	Posudzovanie zhody s Nariadením - komunikácia	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie
8.	Záznam o validácii zakázaných praktík	AI sandbox musí byť implementovaný tak, aby obsahoval validáciu (ne)použitia zakázaných praktík v zmysle zoznamu zakázaných praktík uvedených v Nariadení.	Hlava II.	Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul konfigurácie testovania, validácie a evidencií
9.	Záznam a správa vyhodnotenia rizík systému AI	AI sandbox bude implementovaný tak, aby bolo možné nastaviť a zaznamenávať validáciu v súlade so systémom riadenia rizík a zaznamenávať všetky kroky v rámci posudzovania a testovania jednotlivých systémov	Hlava III.	Posudzovanie zhody s Nariadením - komunikácia	Posudzovanie zhody s Nariadením Konfigurovanie AI sandboxu	Kolaboračný modul Modul konfigurácie testovania, validácie a evidencií

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
				Konfigurovanie systému a pravidiel		
10.	Ochrana osobných údajov	AI sandbox bude implementovaný tak, aby (i) boli všetky osobné údaje vo funkčne oddelenom, izolovanom a chránenom prostredí spracovania údajov pod kontrolou účastníkov, (ii) prístup k týmto údajom mali len oprávnené osoby a (iii) boli splnené ďalšie požiadavky vyplývajúce z Nariadenia a osobitných právnych predpisov na ochranu údajov. Vymazanie údajov po skončení testovania.	Článok 54	Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul pre administráciu a bezpečnosť
11.	Ochrana osobných údajov	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia nasledujúcich oblastí (v rozsahu aplikovateľnom na príslušný systém): zaznamenávanie logov zo spracovania osobných údajov v rámci AI sandboxu počas trvania účasti v AI sandboxe	Článok 53	Posudzovanie zhody s Nariadením - komunikácia	Posudzovanie zhody s Nariadením	Kolaboračný modul Modul pre administráciu a bezpečnosť
12.	Správa údajov a výsledkov testovania	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia nasledujúcich oblastí (v rozsahu aplikovateľnom na príslušný systém):	Článok 53 ods. 1g	Posudzovanie zhody s Nariadením -	Posudzovanie zhody s Nariadením	Kolaboračný modul

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
		- Správa výsledkov testovania/výsledná správa; - Uchovanie úplného a podrobného opisu procesu a dôvodov tréovania, testovania a validácie systému umelej inteligencie a výsledkov; - Umožnenie zdieľania správ z výstupov s inými orgánmi dohľadu nad trhom a posudzovania zhody	Článok 54	komunikácia Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul pre administráciu a bezpečnosť
13.	Posudzovanie zhody s požiadavkami Nariadenia Evidencia zoznamu systémov umelej inteligencie	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia požiadaviek Nariadenia (v rozsahu aplikovateľnom na príslušný systém), vrátane nasledovných: Splnenie požiadaviek na vypracovanie požadovanej technickej dokumentácie v súlade s požiadavkami Nariadenia, vrátane, no bez obmedzenia, nasledovných náležitostí: - Popis prvkov systému umelej inteligencie; - Popis procesu vývoja, metód vývoja, nástrojov poskytnutých tretími stranami a spôsob ich použitia, integrácie a úpravy; - Popis špecifikácie návrhu systému, všeobecná logika systému umelej inteligencie a algoritmov;	Príloha IV	Prihlasovanie do systému Podávanie žiadosti o posúdenie s Nariadením Konfigurovanie systému a pravidiel	Posudzovanie zhody s Nariadením Konfigurovanie AI sandboxu	Kolaboračný modul Modul konfigurácie testovania, validácie a evidencií

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
		• Popis architektúry systému, softvérových komponentov a ich vzťahy; • Opis trénovacích metodík a techník a použitých súborov trénovacích údajov vrátane informácií o pôvode týchto súborov údajov, ich rozsahu a hlavných vlastnostiach; spôsob získavania a výberu údajov • Postupy označovania (napr. pre učenie s učiteľom), metodiky čistenia údajov (napr. zisťovanie odľahlých hodnôt);				
14.	Posudzovanie zhody s požiadavkami Nariadenia	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia požiadaviek Nariadenia (v rozsahu aplikovateľnom na príslušný systém), vrátane nasledovných: Posúdenie opatrení pre zabezpečenie ľudského dohľadu, vrátane posúdenia technických opatrení potrebných na uľahčenie interpretácie výstupov systémov umelej inteligencie príslušnými subjektmi	Príloha IV a Článok 13, 14	Prihlasovanie do systému Posudzovanie zhody s Nariadením - komunikácia	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie
15.	Posudzovanie zhody s požiadavkami	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia požiadaviek Nariadenia (v rozsahu	Článok 13, 20 a 51 a 52 a nasl.	Prihlasovanie do systému	Posudzovanie zhody s Nariadením	Kolaboračný modul

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
	Nariadenia	aplikovateľnom na príslušný systém), vrátane nasledovných: Posúdenie opatrení pre zabezpečenie súladu s požiadavkami na: • Transparentnosť a poskytovanie informácií používateľom; • Uchovávanie logov automaticky generovaných vysokorizikovými systémami AI; • Zabezpečenie registrácie vysokorizikového systému v príslušnej databáze EÚ		Podávanie žiadosti o posúdenie s Nariadením Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Portál a používateľské rozhranie Modul pre administráciu a bezpečnosť
16.	Posudzovanie zhody s požiadavkami Nariadenia	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia požiadaviek Nariadenia (v rozsahu aplikovateľnom na príslušný systém), vrátane nasledovných: Zabezpečenie opisu vopred určených zmien systému AI a jeho výkonnosti spolu so všetkými relevantnými informáciami týkajúcimi sa technických riešení prijatých na zabezpečenie trvalého súladu systému umelej inteligencie s príslušnými požiadavkami stanovenými Nariadením (a ďalšími aplikovateľnými predpismi)	Príloha IV a Hlava III kapitola 2;	Posudzovanie zhody s Nariadením - komunikácia	Posudzovanie zhody s Nariadením	Kolaboračný modul Portál a používateľské rozhranie
17.	Posudzovanie zhody s	AI sandbox bude poskytovať funkcie pre záznam z kontroly a vyhodnotenia	Článok 15	Posudzovanie zhody s	Posudzovanie zhody s Nariadením	Kolaboračný modul

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
	požiadavkami Nariadenia	požiadaviek Nariadenia (v rozsahu aplikovateľnom na príslušný systém), vrátane nasledovných: - Použité postupy validácie a testovania vrátane informácií o použitých validačných a testovacích údajoch a ich hlavných vlastnostiach; - Metriky používané na meranie presnosti, spoľahlivosti a dosiahnutie súladu s inými relevantnými požiadavkami; - Potenciálne diskriminačné vplyvy; testovacie logy a všetky správy o testoch s dátumom a podpisom zodpovedných osôb.	Príloha IV a Hlava III, kapitola 2	Nariadením - komunikácia Konfigurovanie systému a pravidiel	Konfigurovanie regulačného prostredia	Modul konfigurácie testovania, validácie a evidencií
18.	Napojenie na vyhradené rozhranie Komisie pre účely AI sandboxov a jednotné kontaktné miesto EÚ	Nariadenie predpokladá vytvorenie jednotného a vyhradeného rozhrania, ktoré bude obsahovať všetky relevantné informácie týkajúce sa AI sandboxov, spolu s jednotným kontaktným miestom na úrovni EÚ s cieľom komunikovať s AI sandboxmi v členských štátoch a umožniť zainteresovaným stranám klásť otázky príslušným orgánom a žiadať nezáväzné usmernenia o zhode inovačných produktov, služieb a obchodných modelov zahŕňajúcich technológie umelej inteligencie	Článok 53 ods. 6	Zdieľanie metodík, návodov, usmernení a pravidiel	Riadenie regulačného procesu	Kolaboračný modul
19.	Používateľské funkcie	Systém umožní zobrazenie údajov, výstupov v používateľsky prívetivom rozhraní v zmysle Vyhlásky MIRRI č.	§14, §15	Zobrazenie podaných žiadostí,		Portál a používateľské rozhranie

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
		78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy		monitorovanie stavu a údajov		
20.	Používateľské funkcie	Systém umožní zobrazenie údajov prostredníctvom webového prehliadača s definovanými zónami pre neprihlásených alebo prihlásených používateľov. Systém bude disponovať minimálne nasledujúcimi oddelenými typmi vizuálnych zón - zóna žiadateľa, zóna regulátora (zriaďujúceho orgánu) a zóna zúčastnených strán. (ďalšia úroveň prístupu bude nastaviteľná na úrovni používateľských skupín ako aj dát)		Zobrazenie podaných žiadostí, monitorovanie stavu a údajov		Portál a používateľské rozhranie
21.	Administrácia systému	Systém umožní správu používateľov, oprávnení, prístupu k dátam, ich klasifikáciu.		Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul pre administráciu a bezpečnosť
22.	Administrácia systému	Systém umožní monitorovanie, logovanie, reporting a audit používania systému na úrovni vybraných konfigurovateľných používateľských, procesných a systémových udalostí.		Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul pre administráciu a bezpečnosť

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
23.	Administrácia systému	Systém bude implementovaný v súlade s požiadavkami kybernetickej bezpečnosti v zmysle: Vyhlášky MIRRI: č. 179/2020 Z. z., ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy Vyhlášky 362/2018 Z. z. Národného bezpečnostného úradu, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení Zároveň systém bude implementovaný v súlade s internými smernicami kybernetickej bezpečnosti zriaďujúceho orgánu, ktoré budú definované počas fázy prípravy projektu v prostredí konkrétneho OVM.		Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul pre administráciu a bezpečnosť
24.	Administrácia systému	Požiadavky prevádzky a dostupnosti infraštruktúry. Systém bude prevádzkovaný v cloudovom prostredí - produkčné, testovacie a vývojové. Predpokladom je využitie služieb Vládneho cloudu SR.		Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Modul pre administráciu a bezpečnosť

	Popis identifikovaných základných požiadaviek ¹⁰⁹			Mapovanie návrhu budúceho riešenia na požiadavku (popis riešenia je nižšie)		
Por. č.	Skupina požiadaviek (Nariadenie)	Legislatívna požiadavka, ktorú má AI sandbox prostredie" zabezpečiť	Článok Nariadenia	Biznis služba (návrh)	Biznis funkcia alebo proces (návrh)	Modul IS (návrh)
25.	Administrácia systému	Požiadavky na integráciu. Predpokladá sa prepojenie systému v rozsahu: 1. Autentifikácia pri prihlásení pomocou eID uchádzača - prepojenie s IAM. 2. Automatické vyplnenie údajov podľa príslušných registrov verejnej správy: - Register právnických osôb a podnikateľov - Register fyzických osôb Popis účelu: automatické získanie údajov o registrovanom subjekte pri registrácií alebo podávaní žiadosti min. Pre právnické osoby v rozsahu IČO, názov firmy, adresa sídla, štatutári. Pre fyzické osoby - podnikateľov: meno, priezvisko, adresa bydliska		Konfigurovanie systému a pravidiel	Konfigurovanie AI sandboxu	Integračný modul

5.2 Stanovenie variantov technologického riešenia sandboxu pre umelú inteligenciu v zmysle Nariadenia

Pre aplikačnú vrstvu technického riešenia sandboxu je možné uvažovať s nasledovnými alternatívami:

1. **Využitie kancelárskych aplikačných balíkov** - Využitie kancelárskych balíkov pre zabezpečenie spracovania žiadostí (e-mail), záznamu testovania (Excel, Word a pod.) so zverejňovaním výstupov pomocou existujúcich napr. webový portál zriaďovacieho orgánu.
2. **Vybudovanie špecializovaného systému pre správu a podporu AI sandboxu** - vybudovanie nového riešenia, podľa požiadaviek definovaných Nariadením ako aj súvisiacimi právnymi predpismi a požiadavkami zainteresovaných strán. Tento aplikačný variant je možné realizovať nasledovnými technologickými (infraštruktúrnymi) "podvariantmi":
 - a. **Využitie cloudovej infraštruktúry - služby privátneho Vládneho cloudu**
 - b. **Využitie cloudovej infraštruktúry - služby verejného Vládneho cloudu**

Variant vybudovania špecializovaného systému predpokladá nákup implementáciu nového systému, keďže v súčasnej dobe nie je zrejmé, ktorá inštitúcia bude zriaďovateľom resp. dozorným orgánom v oblasti AI v podmienkach Slovenskej republiky.

Tabuľka č.13.: Popis variantov z pohľadu aplikačnej a technologickej vrstvy

Va ria nt	Názov variantu	Popis variantu	Výhody a prínosy variantu	Nevýhody a riziká variantu
1.	Využitie kancelárskych aplikačných balíkov (bez implementácie nového IT riešenia)	Využitie kancelárskych balíkov pre zabezpečenie spracovania žiadostí (e-mail), záznamu testovania (Excel, Word a pod.) so zverejňovaním výstupov pomocou existujúcich napr. Webový portál príslušného zriaďujúceho orgánu	Jednoduchá realizácia sandboxu z projektového pohľadu (založená len na metodicko - organizačných zmenách bez IT zmien) Nízke náklady realizácie	Zložitá udržiateľnosť riešenia Nízka miera zabezpečenia, archivácie údajov a pod. (e-mailová) Nemožnosť automatizovaného riadenia procesu
2a.	Vybudovanie technického riešenia pre podporu AI sandboxu Využitie cloudovej infraštruktúry - služby privátneho Vládneho cloudu	Vybudovanie špecializovaného systému pre správu a podporu AI sandboxu Využitie služieb privátnej časti vládneho cloudu: https://sk.cloud/	Zavedenie štandardizovaných postupov a procesov podporovaných automatizáciou Zabezpečenie spracovania a archivácie údajov Jednotné používateľské rozhranie	Vyššie investičné náklady *
2b.	Vybudovanie technického riešenia pre podporu AI sandboxu Využitie cloudovej infraštruktúry - služby verejného cloudu	Využitie služieb verejnej časti vládneho cloudu: https://katalog.statneit.sk/	Zavedenie štandardizovaných postupov a procesov podporovaných automatizáciou Zabezpečenie spracovania a archivácie údajov Jednotné používateľské rozhranie Prenositelnosť riešenia Lepšia možnosť využitia PaaS služieb	Vyššie investičné náklady *

5.3 Stanovenie kritérií pre výber variantu technologického riešenia podpory AI sandboxu

Navrhované kritériá pre výber vhodného variantu technologického riešenia (pre aplikačnú a technologickú vrstvu) sú zamerané predovšetkým na vyhodnotenie účelu a identifikáciu nevyhnutných súčasti riešenia. Ku kritériám sú navrhnuté váhy expertným posúdením, ktoré primárne zohľadňujú ich relatívnu dôležitosť z pohľadu naplnenia účelu a požiadaviek. Súlad s Nariadením je považovaný za kľúčové kritérium tzv. "KO kritérium". Toto kritérium predstavuje súhrn naplnenia rámcových požiadaviek definovaných v tejto Štúdii. Zdôvodnenie jednotlivých kritérií sa nachádza v tabuľke nižšie. Navrhované kritériá sú následne použité v zjednodušenej multi-kritériálnej analýze.

Tabuľka č.14.: Popis kritérií pre výber variantu z pohľadu aplikačnej a technologickej vrstvy

	KRITÉRIUM	ZDÔVODNENIE KRITÉRIA	Váha kritéria
Aplikačná a technologická vrstva	Súlad s Nariadením a súvisiacou legislatívou (KO kritérium)	Súlad s požiadavkami na technické riešenie pre podporu sandboxu v zmysle požiadaviek Nariadenia	30%
	Využitie súčasnej IT architektúry	Kritérium ktoré zohľadňuje či je možné v prevažnej miere využiť existujúce SW a HW riešenia alebo či je potrebné vyvíjať nové riešenie.	10%
	IT bezpečnosť riešenia	Možnosť zabezpečenia oddeleného spracovania žiadostí údajov, správy používateľov a pod.	20%
	Náklady na IT riešenie (TOC)	Komparatívne porovnanie celkových nákladov na iné varianty (napr. nízke: 3, stredné: 2, vysoké: 1)	10%
	Automatizácia procesu a spracovania údajov a jednotné používateľské rozhranie	Možnosť automatizovaného spracovania žiadostí, správy údajov a komunikácie medzi zainteresovanými stranami, priateľivosť používateľského rozhrania	20%
	Flexibilita riešenia	Modulárnosť a prispôsobiteľnosť riešenia na budúce požiadavky legislatívy pre sandbox.	10%

5.3.1 Multikritériálna analýza pre výber technologického riešenia podpory AI sandboxu

Výber vhodného variantu technologického riešenia podpory AI Sandboxu vychádza predovšetkým z naplnenia požiadaviek na zabezpečenie technickej podpory sandboxu. Pre tento účel boli vyhodnotené jednotlivé navrhované kritériá, na základe nich boli porovnané identifikované varianty.

Vyhodnotenie kritérií v tabuľke nižšie je stanovené na základe určenia hodnoty, ktorého výsledok tvorí vážený priemer v zmysle váh jednotlivých kritérií. Tento model predstavuje kalkulovaný výsledok, na základe ktorého je možné porovnať jednotlivé varianty. Celkové vyhodnotenie variantov sa môže pohybovať v intervale 1 až 3, kde 1 je hodnota pri ktorej variant nespĺňa kritériá a hodnota 3 spĺňa v prevažnej miere. Navrhovaná škála pre vyhodnotenie kritérií resp. predpokladaná miera splnenia kritériá: 1 - Nesplní, 2 - Splní čiastočne a 3 - Splní v prevažnej miere.

Tabuľka č. 15: Multikritériálne vyhodnotenie z pohľadu aplikačnej a technologickej vrstvy

	KRITÉRIUM	Variant 1 Využitie kancelárskych aplikačných balíkov	Variant 2a Vybudovanie technického riešenia pre podporu AI sandboxu Využitie cloudovej infraštruktúry - služby Vládneho cloudu	Variant 2b Vybudovanie technického riešenia pre podporu AI sandboxu Využitie cloudovej infraštruktúry - služby privátneho cloudu
Aplikačná a technolog ická vrstva	Súlady s Nariadením a súvisiacou legislatívou (KO)	2 - Splní čiastočne	3 - Splní v prevažnej miere	3 - Splní v prevažnej miere
	Využitie súčasnej IT architektúry	3 - Splní v prevažnej miere	2 - Splní čiastočne	2 - Splní čiastočne
	IT bezpečnosť riešenia	2 - Splní čiastočne	3 - Splní v prevažnej miere	3 - Splní v prevažnej miere
	Náklady na IT riešenie (TOC)	3 - Splní v prevažnej miere	2 - Splní čiastočne	2 - Splní čiastočne
	Automatizácia procesu a spracovania údajov a jednotné používateľské rozhranie	1 - Nesplní	3 - Splní v prevažnej miere	3 - Splní v prevažnej miere
	Výsledok (vážený priemer) Vyššie skóre predpokladá vhodnejšie riešenie v intervale 1 až 3.	1,9	2,8	2,8

5.3.2 Návrh odporúčania budúceho variantu aplikačnej a technologickej vrstvy technologického riešenia AI na základe kritérií

Z pohľadu vyššie definovaných kritérií sa javí ako optimálna aplikačná a technologická alternatíva **Vybudovanie technického riešenia pre podporu AI sandboxu s podvariantmi využitia verejnej alebo privátnej časti Vládneho cloudu.**

Navrhované riešenie bude predstavovať jednotný systém, ktorý pri správnom návrhu splní legislatívne požiadavky dané Nariadením, zabezpečí flexibilitu, bezpečnosť údajov ako aj riadenie procesu testovania a komunikácie medzi zainteresovanými stranami.

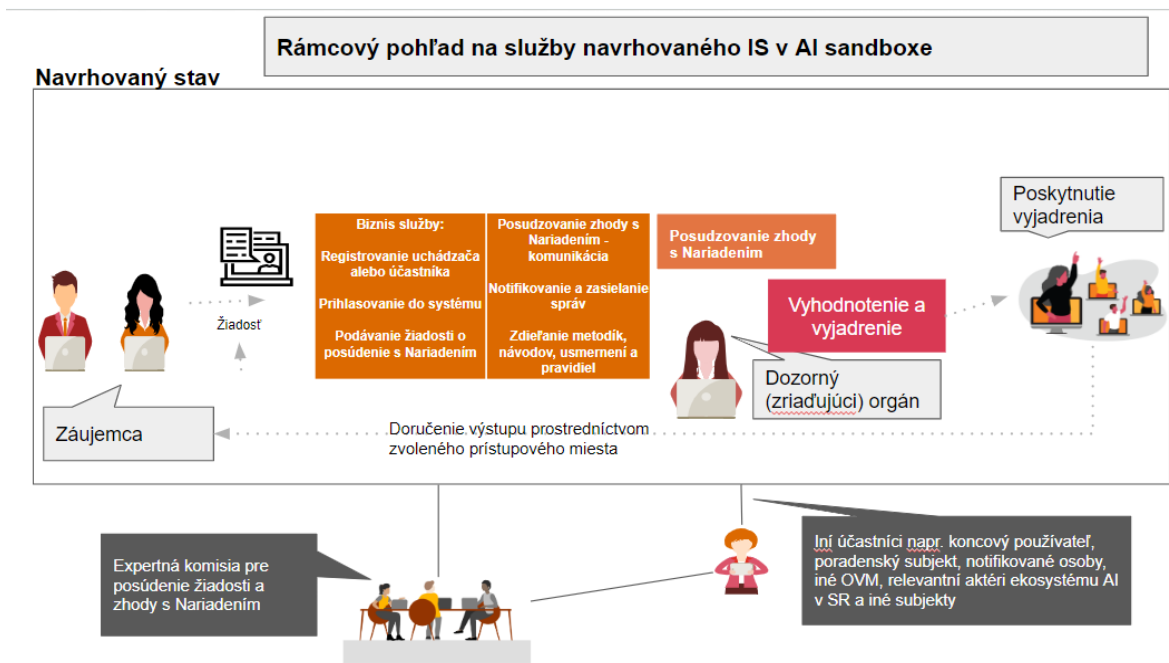
Nevýhodou riešenia budú vyššie obstarávacie náklady v porovnaní s alternatívnym riešením, ktoré sú však nevyhnutné investovať pre naplnenie požiadaviek, ktoré sú sumarizované v rámci vyššie uvedených častí Štúdie a je ich možné potenciálne znížiť využitím existujúcich platforiem (workflow management, document management, portál a pod.) v závislosti od inštitúcie, ktorá bude vlastniť a spravovať budúci systém.

5.4 Základné používateľské prípady

Navrhované riešenie pre podporu AI sandboxu (pracovný názov IS AIRS - Artificial Intelligence Regulatory Sandbox) je z pohľadu funkčnosti založené na legislatívnych a používateľských požiadavkách, ktoré vychádzajú zo súčasného popisu potrieb a povinností v Nariadení ako aj z “best practices”, ktoré sú využívané pri návrhu informačných systémov.

Pre vykonávanie používateľských prípadov boli navrhnuté “biznis služby”, ktoré podporujú dosiahnutie želaného výstupu z pohľadu používateľov.

Obrázok č.4.: Rámcový pohľad na služby navrhovaného IS v AI sandboxe



Na základe doposiaľ identifikovaných požiadaviek je možné navrhnuť rámcový popis kľúčových **používateľských prípadov** navrhovaného riešenia pre:

1. registráciu žiadateľa,
2. podanie žiadosti o posúdenie zhody AI riešenia s Nariadením,
3. posudzovanie zhody s požiadavkami Nariadenia.

Tieto používateľské prípady predstavujú ilustratívny pohľad na niektoré časti fungovania navrhovaného systému, nepredstavujú podrobný procesný návrh. **Procesný návrh, ako aj definíciu ďalších používateľských prípadov odporúčame realizovať v rámci tvorby funkčnej a technickej špecifikácie riešenia resp. detailného návrhu riešenia, po ustálení znenia Nariadenia.**

1. Registrácia do IS AIRS - z pohľadu záujemcu, ktorý je žiadateľom:

- Žiadateľ bude pristupovať cez webové rozhranie - portál
- Pred podaním žiadosti, bude potrebná registrácia v IS AIRS
- Žiadateľ sa bude registrovať elektronicky, pomocou prihlásenia eID a vyplnenia registračného formulára
- Registračný formulár bude intuitívny a bude vyžadovať len nevyhnutné údaje. Údaje žiadateľa (meno, adresa, IČO a pod.) budú dotiahnuté z RPOaP prípadne RFO.
- Po registrácii sa bude môcť žiadateľ prihlásiť a následne spustiť proces podania žiadosti o posúdenie

2. Podanie žiadosti o vstup do AI sandboxu - z pohľadu záujemcu, ktorý je žiadateľom:

- Prihlásený žiadateľ podá žiadosť prostredníctvom preddefinovaného formulára
- Žiadosť bude zvalidovaná (prijatá a sprioritizovaná) expertmi, ktorých nominuje zriaďujúci orgán, a ktorí rozhodnú o ďalších krokoch v posudzovaní v zmysle stanovenej metodiky resp. nastaveného pracovného toku.
- Posudzovanie zhody - priebeh posudzovania zhody s požiadavkami Nariadenia bude v IS AIRS nastaviteľný flexibilne v zmysle neskorších fáz projektu a bude reflektovať aktuálne ustanovenia príslušných predpisov, nastavenú metodiku a pravidlá prevádzky sandboxu.
- Operatívna komunikácia pri prioritizácii alebo posudzovaní bude prebiehať prostredníctvom portálu IS AIRS, v ktorom bude mať používateľ zriadenú zónu žiadateľa s vytvorenými validačnými resp. testovacími zónami.
- O jednotlivých krokoch procesu bude používateľ informovaný notifikáciami (na emailovú adresu), údaje o akýchkoľvek prípadných úradných rozhodnutiach budú doručené aj do Elektronickej schránky.
- Všetky údaje o žiadosti, testovaní a validácii budú ukladané v oddelenom chránenom úložisku s riadeným prístupom k dátam.

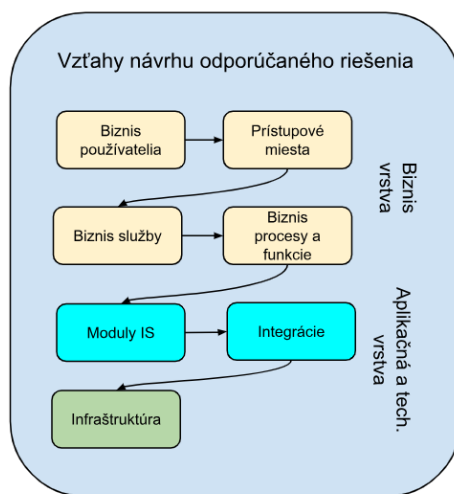
3. Posudzovanie zhody s požiadavkami Nariadenia - z pohľadu zriaďovateľa sandboxu pre umelú inteligenciu a správcu systému:

- Posudzovanie zhody bude možné začať po podaní a elektronickom doručení žiadosti uchádzačom prostredníctvom webového portálu
- Žiadosť bude zvalidovaná na základe preddefinovaných kritérií a zaznamenaná v systéme
- Žiadateľ bude po kladnom posúdení žiadosti vyzvaný na spoluprácu pri testovaní a poskytovaní vstupných údajov, dokumentov a technických prostriedkov

- Správca systému vytvorí v IS AIRS prostredie pre záznam z validácie, kde zhromaždí vstupné údaje, údaje o validácii, komunikácii medzi zúčastnenými stranami (vrátane prípadných ostatných zúčastnených OVM a iných aktérov) ako aj údaje o výstupoch posudzovania.
- Po ukončení procesu posudzovania bude žiadateľ notifikovaný o výsledku (napr. e-mailom alebo doručením do Elektronickej schránky) pričom všetky údaje zostanú zaznamenané po dobu určenú právnymi predpismi.

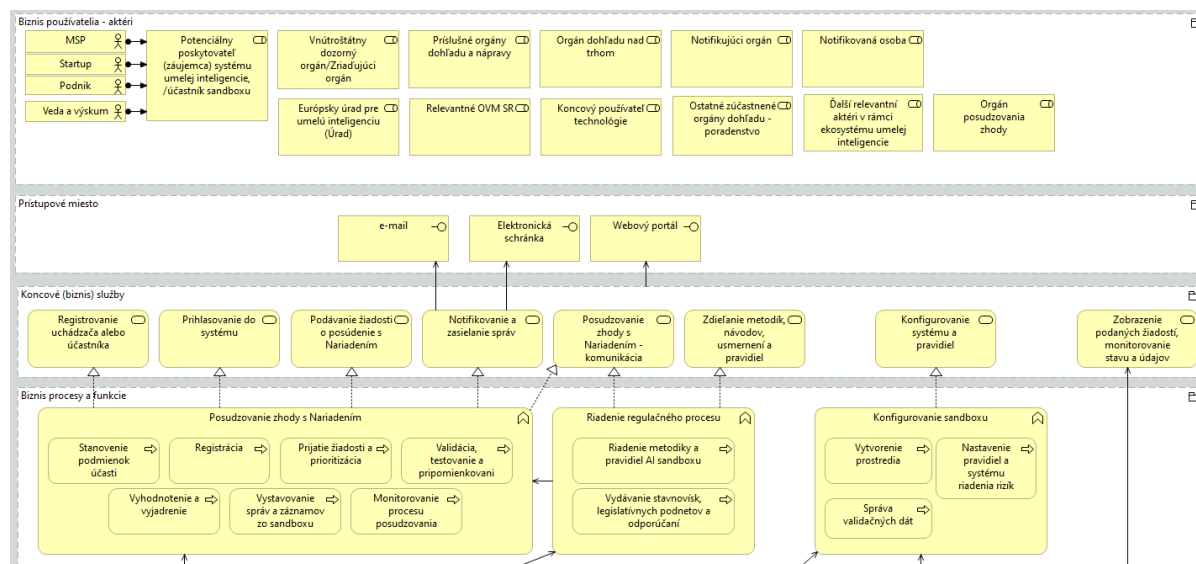
Pre podporu vykonávania používateľských prípadov je navrhnuté komplexné riešenie, ktoré sa skladá z častí uvedených na nasledujúcom obrázku. Tieto časti sú vzájomne prepojené tak, že biznis používatelia (1.) resp. aktéri prístupujú do systému prostredníctvom prístupových miest (2.) k používateľským biznis službám. Biznis služby (3.) vyplývajú z funkcií a procesov (4.), ktoré prebiehajú v rámci organizácie. Technologicky sú podporované aplikačnou vrstvou - t.j. modulmi IS a integráciami a infraštruktúrou.

Obrázok č.5.: Vzťahy návrhu odporúčaného riešenia



Nasledujúci obrázok popisuje biznis vrstvu navrhovaného riešenia, v ktorej sú popísané navrhované súčasti ako napr. biznis používatelia, prístupové miesta, koncové služby, biznis procesy a funkcie.

Obrázok č.6.: Rámcový návrh biznis architektúry riešenia pre podporu AI Sandboxu



Jednotlivé časti biznis architektúry sú popísané v nasledujúcom texte:

1. **Biznis používateľia** - používateľské skupiny, ktoré vychádzajú z definície podľa kapitoly 2.1. tejto štúdie
2. **Prístupové miesta** - predstavujú rozhrania pre používateľský prístup a komunikáciu:
 - a. **Webový portál** - základný prístup do systému pre všetky typy používateľov podľa nastaviteľných oprávnení. Prístup k používateľským biznis službám
 - b. **E-mail** - zasielanie notifikácií o priebehu
 - c. **Elektronická schránka** - zasielanie záväzných rozhodnutí napr. vyjadrenie o výsledku posúdenia
3. **Koncové (biznis) služby** - Tieto služby podľa definície, naplňajú určitú potrebu používateľa pri komunikácii s verejnou správou. V prípade tohto návrhu sú to používateľské služby, ktoré reflektujú legislatívne a používateľské požiadavky na technické zabezpečenie AI sandboxu.

P.č.	Biznis služby (používateľské služby)
1.	Registrowanie uchádzača alebo účastníka
2.	Prihlasovanie do systému
3.	Podávanie žiadosti o prístup do sandboxu pre účely posúdenia zhody s Nariadením
4.	Notifikovanie a zasielanie správ
5.	Posudzovanie zhody s požiadavkami Nariadenia - komunikácia
6.	Zdieľanie metodík, návodov, usmernení a pravidiel
7.	Konfigurovanie systému a pravidiel
8.	Zobrazenie podaných žiadostí, monitorovanie stavu a údaj

4. **Biznis funkcie a procesy**, predstavujú popis hlavných funkcií a procesov organizácie, cieľom funkcií a služieb je poskytovanie biznis služieb používateľom.

P.č.	Biznis funkcia AI sandboxu	Biznis procesy AI sandboxu
1.	Posudzovanie zhody s Nariadením	Stanovenie podmienok účasti Registrácia Prijatie žiadosti a prioritizácia Validácia, testovanie a pripomienkovanie Vyhodnotenie a vyjadrenie Vystavovanie správ a záznamov zo sandboxu Monitorovanie procesu posudzovania zhody s Nariadením
2.	Riadenie regulačného procesu	Riadenie metodiky a pravidiel AI sandboxu Vydávanie stanovísk, legislatívnych podnetov a odporúčaní
3.	Konfigurovanie sandboxu	Vytvorenie prostredia Nastavenie pravidiel a systému riadenia rizík Správa validačných dát

Pre zabezpečenie fungovania biznis služieb, funkcií a procesov navrhujeme moduly informačného systému t.j. softvérové aplikácie ako aj súvisiacu infraštruktúru, na ktorej by mal byť prevádzkovaný informačný systém. Návrh základných blokov informačného systému pre podporu AI sandboxu je popísaný v ďalšej kapitole.

5.5 Návrh technického riešenia podpory sandboxu pre umelú inteligenciu v zmysle Nariadenia z pohľadu požiadaviek

Princípy návrhu technického riešenia IS AIRS sú:

- návrh je realizovaný na základe dostupného znenia Nariadenia,
- úroveň granularity návrhu umožňuje jeho prispôsobenie do budúcnosti,
- požiadavky na služby a popisy sú z popísané z pohľadu zadávateľa riešenia a na základe dostupných dokumentov (podrobný zber požiadaviek nebol v tejto fáze realizovaný),
- návrh obsahuje len aplikačné moduly nevyhnutné pre podporu sandboxu,
- návrh je "dodávateľský neutrálny" - moduly riešenia je možné implementovať rôznou kombináciou softvérových produktov alebo vývojom. Návrh nepredpisuje implementačný postup konkrétneho riešenia ani softvérovú architektúru pre jeho vývoj. Návrh konkrétneho riešenia bude predložený vo fáze výberu dodávateľa riešenia.

Aplikačná a technologická vrstva

Aplikačná vrstva - popis modulov IS a aplikačných služieb, ktoré softvérovo podporia vykonávanie biznis služieb, procesov a funkcií AI sandboxu:

P.č.	Moduly aplikačnej architektúry IS
1.	Kolaboračný modul
2.	Modul konfigurácie testovania, validácie a evidencií
3.	Modul pre administráciu a bezpečnosť
4.	Portál a používateľské rozhranie
5.	Integračný modul

Popis modulov a aplikačných služieb je uvedený v **Tabuľke č. 16** nižšie.

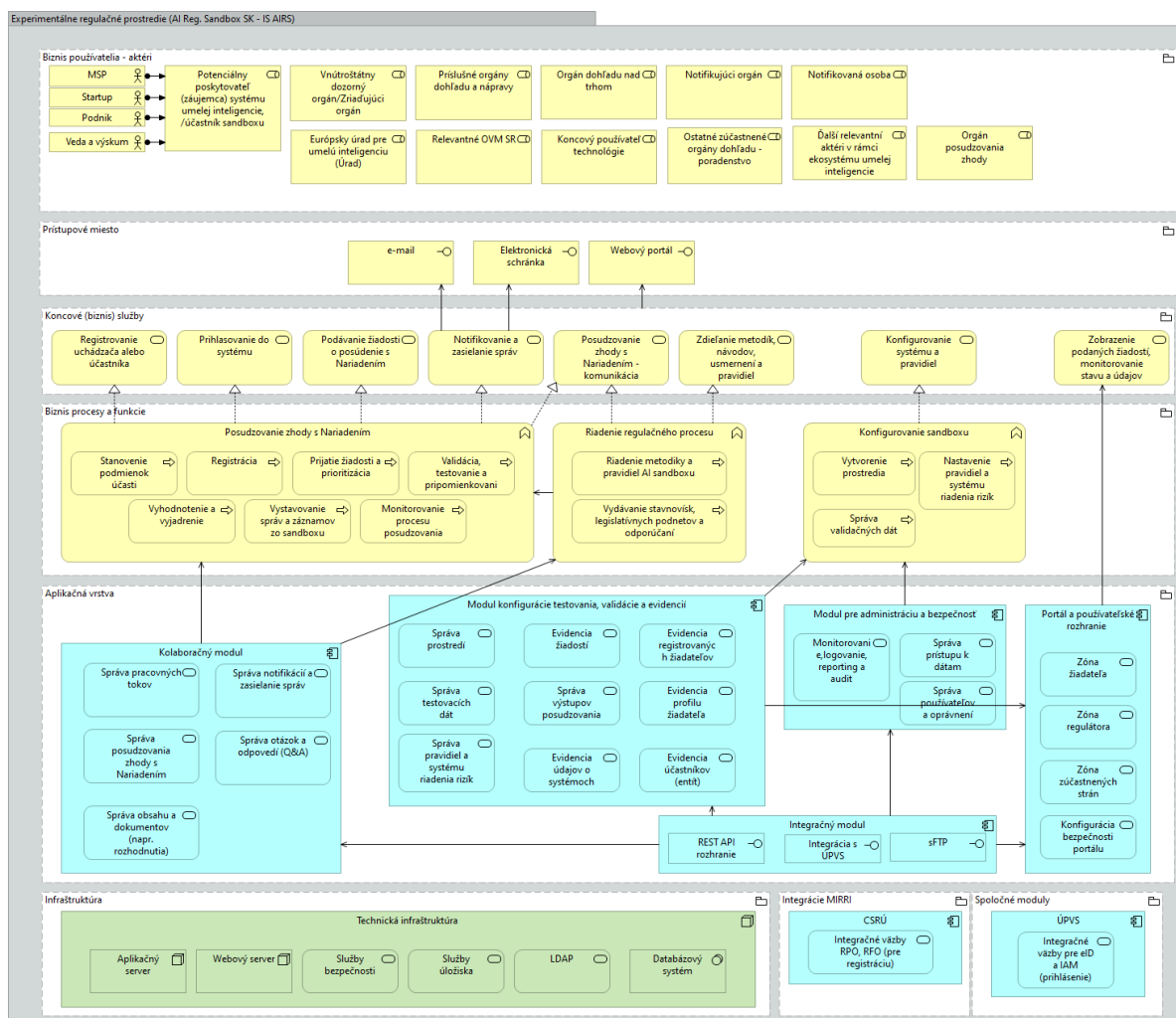
Tabuľka č. 16 Návrh a popis modulov informačného systému IS AIRS, ktoré zabezpečia podporu výkonu experimentálneho regulačného prostredia

Modul informačného systému (návrh)	Popis aplikačných služieb modulu (návrh)
Kolaboračný modul	Modul, ktorý umožňuje kolaboráciu účastníkov, najmä spustenie a monitorovanie pracovných tokov, ktorý je prístupný prostredníctvom používateľského rozhrania prostredníctvom modulu: Portál a používateľské rozhranie. Správa procesu posudzovania zhody s Nariadením, pravidiel, notifikácie, dokumentácie pre výstupy a výstupy vyhodnotenia. 1. Záznam o priebehu pracovných tokov 2. Záznamy z priebehu posudzovania zhody 3. Správa notifikácií a zasielanie správ 4. Správa otázok a odpovedí (Q&A) 1. Interaktívne nastavenie pracovných tokov (workflow) podľa definovaných pravidiel (business rules) s možnosťou parametrizácie, konfigurácie vizuálnym spôsobom bez potreby programovania (napr. low-code, no-code) napr. 1. Stanovenie podmienok účasti 2. Prijatie žiadosti a prioritizácia 3. Validácia a testovanie 4. Vyhodnotenie 5. Vydávanie výsledkov a správ 6. Monitorovanie procesu posudzovania zhody s Nariadením Konfigurácia pravidiel a parametrov je spravovaná v Module konfigurácie testovania, validácie a evidencií 2. Správa priebehu posudzovania zhody: záznamy z priebehu posudzovania zhody a vyhodnotenie podľa pravidiel 3. Správa obsahu a dokumentov (napr. rozhodnutia): správa (uloženie, presun, zamazanie, evidencia, metadáta) dokumentov, vstupných testovacích údajov, obrázkov, záznamov o priebehu, výsledkov validácie, rozhodnutí a pod. 4. Správa notifikácií a zasielanie správ: • Zasielanie notifikácií o priebehu testovania v rámci definovaného workflow • Záznam komunikácie a správ medzi zúčastnenými stranami 5. Správa otázok a odpovedí (Q&A): Zaznamenávanie otázok a odpovedí od uchádzačov
Modul konfigurácie testovania, validácie a evidencií	Modul je určený predovšetkým pre konfiguráciu a vytvorenie testovacích prostredí, správu a evidenciu dát a systému riadenia rizík, výstupov validácie, verzionovania a pod. • Konfigurácia prostredí • Konfigurácia ochrany testovacích dát (napr. vstupných datasetov) • Konfigurácia pravidiel výstupov posudzovania (napr. nastavenie kontrolného checklistu) • Konfigurácia systému riadenia rizík • Konfigurácia pre validáciu autorských práv, • Zabezpečenie úložiska a jeho oddelenie. Modul umožní správu záznamov o registráciách, profiloch a žiadostiach, ktoré boli zaregistrované v rámci pracovných tokov, poskytovaných Kolaboračným modulom: • Evidencia žiadostí • Evidencia registrovaných žiadateľov • Evidencia profilu žiadateľa

Modul informačného systému (návrh)	Popis aplikačných služieb modulu (návrh)
	- Evidencia účastníkov (entít) - Evidencia údajov o systémoch
Modul pre administráciu a bezpečnosť	Modul umožní nastavenie systémovej správy a bezpečnosti v rozsahu: - Monitorovanie, logovanie, auditovanie a reportovanie udalostí - Manažérsky reporting a kategorizované štatistiky o udalostiach (interný a externý) - Umožní monitorovanie, logovanie a audit používateľských, procesných a systémových udalostí, ktoré je možné nakonfigurovať - Poskytne prehľad a reporting pre monitorovanie, logovanie a audit - Poskytne prehľad a reporting zoznamu používateľov, skupín, zmeny v nastaveniach oprávnení, časové záznamy zmien a pod. Správa prístupu používateľov k dátam (evidenciám, obrazovkám a pod): - Nastavenie prístupu k dátam podľa kategórií, vlastníka, profilu a pod. - Nastavenie ochrany pred neoprávneným prístupom - Nastavenie klasifikácie údajov (osobné údaje, citlivé údaje a pod.) - Nastavenie parametrov metadát a pohľadu ochrany osobných údajov, napr. zdroj, doba uloženia, účel a pod. Správa používateľov a oprávnení: - Nastavenie prístupu - Správa používateľov a používateľských skupín - Nastavenie oprávnených osôb - Vytvorenie, zmena, aktivácia, deaktivácia a vymazanie používateľa. - Vytvorenie, zmena, aktivácia, deaktivácia a vymazanie používateľských skupín a rolí. - Nastavenie používateľských a prístupových práv.
Portál a používateľské rozhranie	Front-end systému, ktorý sa skladá z portálu a prezentačnej vrstvy, ktoré je prístupná používateľom v rôznych režimoch. Prístupový bod pre používateľov z interného a externého prostredia by mal byť rozdelený minimálne do nasledujúcich zón: - Zóna žiadateľa: prístup len do určenej zóny resp. zón pre zistenie priebehu, komunikáciu a výstupy hodnotenia a validácie. - Zóna hodnotiteľa (technickí experti, vedci a pod.): prístup len do určenej zóny pre zistenie priebehu, komunikáciu a prípravu výstupov hodnotenia a validácie. - Zóna regulátora: používateľský prístup do všetkých zón na základe interných pravidiel - Konfigurácia bezpečnosti portálu na základe princípu segregation of duties, určená pre administrátora bezpečnosti IS AIRS
Integračný modul	Poskytne integračné rozhranie pre nasledujúce integrácie - Integrácia sFTP pre výmenu súborov (napr. Testovacie dáta) - REST API - pre podporu aplikačnej integrácie Externé integrácie - Integrácia na externé systémy v rámci verejnej správy SK: Pre zjednodušenie procesu registrácie a žiadosti je odporúčané využitie údajov, ktorými už v verejná správa disponuje, pomocou integrácie s relevantnými modulmi ÚPVS. Nasledovné integrácie (nice-to-have): - Registrácia používateľa - integrácia - eID, IAM a eSchránka - Dôvod: použitie údajov o žiadateľovi pre identifikáciu (eID a IAM) - Komunikácia s používateľom prostredníctvom eSchránky - Proces žiadosti - integrácia s CSRÚ - Použitie údajov pri predkladaní žiadosti, použitie údajov (adresa, názov firmy a pod.) z údajov registra RPOaP.

Modul informačného systému (návrh)	Popis aplikačných služieb modulu (návrh)
Technická Infraštruktúra	Technická a dátová infraštruktúra, potrebná pre zabezpečenie fungovania systému. Základné prvky infraštruktúry systému: • Aplikačný server • Webový server • Databázový server • Úložisko • Služby správy dát • Služby bezpečnosti a riadenia prístupu

Obrázok č.7.: Celkový pohľad na architektúru návrhu riešenia IS AIRS



5.6 Prehľad nákladovej štruktúry pre zvolenú alternatívu a analýza nákladov na implementáciu a prevádzku sandboxu pre umelú inteligenciu (v zmysle Nariadenia)

Predpokladané náklady na implementáciu a prevádzku riešenia budú pozostávať z organizačného zabezpečenia, investícií a prevádzky technického zabezpečenia ako ostatných administratívnych a iných súvisiacich nákladov. Celkové náklady sa však v budúcnosti môžu líšiť v závislosti od rozsahu a podrobnosti a miery povinnosti plnenia regulačných pravidiel, komplexity technologických potrieb a rýchlosti implementácie.

Je dôležité mať na pamäti, že financovanie regulačného sandboxu pre umelú inteligenciu by malo byť zohľadnené v rámci širšieho plánu vlády alebo regulačného orgánu, aby sa zabezpečilo dlhodobé fungovanie a udržateľnosť projektu.

Tabuľka č.17. : Návrh nákladovej štruktúry

	Nákladová oblasť	Podoblasť	Popis
1	Organizačné zabezpečenie (podľa požiadaviek uvedených v časti 4.3 správy)	Personálne zabezpečenie	- Platy odborníkov (zodpovedných za riadenie, implementáciu a monitorovanie sandboxu) - Financovanie - Možné školenia a vzdelávanie personálu týkajúce sa AI a regulácie
		Administratívne náklady	Náklady na vykonávanie administratívnych úloh, vrátane manažmentu projektu, správy dokumentácie a pod.
2	Technologické náklady (podľa požiadaviek uvedených v časti 5.1 správy)		- Nákup softvéru a technologických nástrojov potrebných na testovanie a overovanie AI - Náklady na vytvorenie vývojového prostredia sandboxu - Náklady na prevádzku technologického riešenia
3	Iné podporné služby	Prípravné práce a štúdie	- Financovanie analýz potrebných na identifikáciu rizík a príležitostí v rámci regulácie AI - Náklady na konzultácie s odborníkmi a zúčastnenými stranami
		Marketing a komunikácia	Náklady na informovanie verejnosti, inštitúcií a podnikov o regulácii AI a o prínosoch sandboxu
		Poradenské služby	- Právne poradenstvo - Iné poradenské služby

Odhadované náklady na implementáciu a prevádzku AI sandboxu predstavujú orientačný pohľad na finančné ohodnotenie, ktorý môže slúžiť na predbežnú alokáciu a plánovanie zdrojov. Reálnejší odhad nákladov bude známy po upresnení legislatívnych a používateľských požiadaviek, ktoré odporúčame realizovať v rámci ďalšej fázy v rámci prípravy funkčnej a technickej špecifikácie a následného výberu dodávateľa riešenia.

5.6.1 Organizačné zabezpečenie

Pre zabezpečenie fungovania organizácie AI sandboxu sa predpokladá zostaviť tím expertov, ktorí budú zodpovední za úlohy, ktoré vyplývajú z Nariadenia a súvisiacej prevádzky.

- Personálne zabezpečenie predstavujú náklady na interných zamestnancov, ktoré sú nad rámec projektu realizácie technického (IT) riešenia.
- Odhadované dedikované ročné interné kapacity na fungovanie AI sandboxu (podľa časti 4.3 správy) predpokladáme v rozsahu 5 resp. 8 zamestnancov.
- Administratívne náklady sú náklady na vykonávanie administratívnych úloh, vrátane manažmentu projektu, správy dokumentácie a pod.

Náklady na externé kapacity sú uvedené v časti **5.5.4 Zhrnutie a prehľad odhadovaných nákladov**.

5.6.2 Technologické náklady

Indikatívna kalkulácia nákladov vychádza z identifikovaných požiadaviek, navrhovaných modulov a odhadu náročnosti vývoja riešenia v zmysle štruktúry nákladovo-výnosovej metodiky, dostupnej na: <https://mirri.gov.sk/sekcie/informatizacia/riadenie-kvality-qa/>.

Kalkulácia v tejto časti zahŕňa vytvorenie technologického riešenia a súvisiaci projekt, náklady na zriadenie organizačného útvaru (napr. interní zamestnanci, priestory a iný materiál) nie sú uvádzané v tejto časti.

Udržateľnosť riešenia je kalkulovaná z dôvodu experimentálnej povahy riešenia na 5 rokov. Odporúčame prehodnotiť prevádzkové náklady a udržateľnosť riešenia priebežne resp. po 3 rokoch, keďže podmienky a technologický vývoj sa môže v tejto oblasti výrazne zmeniť.

Odhad kalkulácie nákladov na realizáciu vychádza z požiadaviek odvodených od aktuálne známej verzie Nariadenia, pričom v blízkej budúcnosti predpokladáme ďalšie spresňovanie a aktualizáciu regulácie v tejto oblasti. **Odporúčame preto realizovať detailnú analýzu požiadaviek, so zohľadnením pripomienok jednotlivých zúčastnených strán po finálnom schválení Nariadenia, pravidelnú revíziu požiadaviek oproti zmenám v znení Nariadenia a následne aj prekalkulovanie súvisiacich nákladov.**

Tabuľka č.18.: Pohľad na náklady na implementáciu IT riešenia pre technickú podporu sandboxu (neobsahuje ďalšie náklady na organizačné zabezpečenie)

	Spolu	Kolaboračný modul	Modul konfigurácie testovania, validácie a evidencií	Modul pre administráciu a bezpečnosť	Portál a používateľské rozhranie	Integračný modul
Náklady s DPH	867 885 €	426 221 €	127 030 €	121 910 €	95 895 €	96 829 €
Všeobecný materiál	- €	- €	- €	- €	- €	- €
IT - CAPEX	589 315 €	326 022 €	76 536 €	74 177 €	55 922 €	56 658 €
Aplikácie	454 315 €	294 022 €	51 536 €	46 177 €	30 922 €	31 658 €
SW	135 000 €	32 000 €	25 000 €	28 000 €	25 000 €	25 000 €
HW	- €	- €	- €	- €	- €	- €
IT - OPEX	244 010 €	82 941 €	45 307 €	43 246 €	36 184 €	36 332 €
Aplikácie	77 010 €	45 941 €	10 307 €	8 246 €	6 184 €	6 332 €
SW	42 000 €	12 000 €	10 000 €	10 000 €	5 000 €	5 000 €
HW	125 000 €	25 000 €	25 000 €	25 000 €	25 000 €	25 000 €
Riadenie projektu	34 560 €	17 258 €	5 186 €	4 488 €	3 789 €	3 839 €

Tabuľka č.19.: Náklady na vývoj a prevádzku z pohľadu časovej štruktúry

Tabuľka predstavuje predpokladané časové rozloženie nákladov pre implementáciu technologického riešenia a neobsahuje prípravnú časť a ani ostatné náklady. Rok 1 (t1) v zmysle tabuľky nižšie, môže nastať až po legislatívnej, organizačnej príprave a následnom obstaraní dodávateľa pre implementáciu IT riešenia. Riadenie projektu je kalkulované ako separátna položka a môže byť využitá pri externom zabezpečení projektového riadenia na strane objednávateľa.

TO BE	Spolu	t1	t2	t3	t4	t5	t6
SW produkty - sumár obstaranie	100 000	100 000	0	0	0	0	0
SW produkty - sumár prevádzka	77 000	0	15 400	15 400	15 400	15 400	15 400
Aplikácie - sumár obstaranie	308 040	308 040	0	0	0	0	0
Aplikácie - sumár prevádzka	223 285	0	44 657	44 657	44 657	44 657	44 657
SW a Aplikácie - výstupné náklady	0	0	0	0	0	0	0
HW sumár obstaranie	0	0	0	0	0	0	0
HW sumár prevádzka	125 000	25 000	25 000	25 000	25 000	25 000	0
Riadenie projektu	34 560	34 560	0	0	0	0	0
Spolu	867 885	467 600	85 057	85 057	85 057	85 057	60 057

5.6.3 Iné podporné služby

Počas realizácie projektu ako aj prevádzky AI sandboxu sa predpokladá využitie odborných a poradenských služieb v oblastiach, kde nie je potrebné alebo efektívne udržiavať interné kapacity. Pôjde najmä o právne stanoviská v oblasti súladu s aktuálnou legislatívou, poradenstvo v oblasti aktuálnych trendov v oblasti umelej inteligencie, strojového učenia, dátového manažmentu, nastavenia postupov pri ochrane dát, zabezpečenie koordinácie testovania a podobne.

Predpokladaný počet človekodní na experta je 100 za rok pre implementáciu, so zameraním najmä na prípravnú časť napr. legislatívna podpora, tvorba metodík a postupov. Po ukončení projektu tzn. počas prevádzky riešenia bude externé zabezpečenie podpory zamerané najmä na konzultácie v oblasti testovania technológií umelej inteligencie, prípravu stanovísk a zmien v lokálnych pravidlách, ako aj na vykrytie kapacít pri prípadnom náraste žiadateľov o posúdenie riešenia.

Tabuľka č.20.: Náklady na podporné služby súvisiace s prevádzkou sandboxu

Typ prevádzkového nákladu	Potrebné kapacity	Odhadované náklady na 1 rok fungovania (EUR)
Iné podporné služby - náklady na externé zabezpečenie	Podporné právne poradenské služby, iné poradenské služby	240 000

5.5.4 Zhrnutie a prehľad odhadovaných nákladov

Predpokladané celkové náklady na realizáciu projektu a celkové zriadenie organizácie zobrazuje **Tabuľka č. 21: Sumár investičných nákladov**. Odhad ročných prevádzkových nákladov sa nachádza v **Tabuľke č. 22: Sumár predpokladaných ročných prevádzkových nákladov - po projekte**:

V oboch prípadoch sú tieto náklady rozčlenené na interné a externé:

- Interné náklady obsahujú kalkuláciu personálnych nákladov na interných zamestnancov organizácie.
- Pri externých nákladoch sú uvedené najmä náklady na projekt implementácie, ktorý by mal byť dodávaný externým IT dodávateľom, ako aj predpokladanú sumárnu alokáciu nákladov na odborné poradenské služby najmä v oblasti umelej inteligencie, práva, prípadne manažmentu dát, ktoré predpokladáme čerpať postupne na základe reálnej potreby organizácie (napr. prostredníctvom rámcových zmlúv, objednávok a pod.)

V rámci položiek investičných nákladov sú zahrnuté náklady na implementáciu nového informačného systému. Prípadné rozšírenie existujúcich systémov nebolo uvažované, nakoľko v súčasnej dobe nie je známa inštitúcia, ktorá bude zriaďujúcim alebo dozorným orgánom.

Odporúčame preto prehodnotiť mieru využitia súčasných prvkov IT architektúry následne po schválení legislatívy, ktorá stanoví zriaďujúci a dozorný orgán pre AI sandbox. Týmto postupom je v budúcnosti možné prehodnotiť celkovú náročnosť implementácie.

Tabuľka č.21.: Sumár investičných nákladov - celkové predpokladané náklady na projekt

Nákladová oblasť - Investície (náklady na projekt)	Typ investičného nákladu	Interné náklady (EUR)	Externé náklady (EUR)	Interné a externé (EUR)
Organizačné zabezpečenie	Personálne zabezpečenie (Rok 1 a 2)	205 324	0	205 324
Organizačné zabezpečenie	Administratívne náklady (Rok 1)	0	10 000	10 000
Technologické náklady	Nákup SW a technológií, implementácia IT riešenia (Rok 2, s rozvojom počas doby udržateľnosti)	0	589 315	589 315
Iné podporné služby	Prípravné práce a štúdie, poradenské, právne služby a riadenie kvality (Rok 1)	0	240 000	240 000
Spolu		205 324	839 315	1 044 639

Tabuľka č.22.: Sumár predpokladaných ročných prevádzkových nákladov - po projekte

Nákladová oblasť - Prevádzka (ročné náklady po projekte)	Typ prevádzkového nákladu (ročne)	Interné náklady (EUR)	Externé náklady (EUR)	Interné a externé (EUR)
Organizačné zabezpečenie	Personálne zabezpečenie	326 408	0	326 408
Organizačné zabezpečenie	Administratívne náklady	0	5 000	5 000
Technologické náklady	Prevádzka SW a technológií	0	48 802	48 802
Iné podporné služby	Marketing a komunikácia	0	1 000	1 000
Iné podporné služby	Prípravné práce a štúdie, poradenské a právne služby	0	240 000	240 000
Spolu		326 408	294 802	621 210

5.7 Časový rámec

Predpokladaný časový rámec vychádza z aktivít, potrebných pre organizačné zabezpečenie a súvisiacej technickej podpory. V nasledujúcej tabuľke sa nachádza prehľad aktivít, ktoré je potrebné realizovať pre vytvorenie sandboxu s predpokladaným trvaním.

Tabuľka č.23.: Časový prehľad odhadovaných nákladov na prípravu a implementáciu AI sandboxu

	Projekt - Príprava sandboxu	Projekt Implementácia sandboxu	Prevádzka					Spolu
	Rok 1 - investičné náklady	Rok 2 - investičné náklady	Rok 3 - prevádzkové náklady	Rok 4 - prevádzkové náklady	Rok 5 - prevádzkové náklady	Rok 6 - prevádzkové náklady	Rok 7 - prevádzkové náklady	Spolu (investičný náklad a prevádzka)
Odhad nákladov na AI sandbox	455 324	794 639	621 210	621 210	621 210	621 210	621 210	4 356 015

- V Roku 1 predpokladáme investičné náklady v hodnote 455 324 Eur, ktoré zahŕňajú interné náklady na personálne zabezpečenie v hodnote 205 324 Eur, externé náklady na prípravné práce a štúdie (napr. právne a poradenské služby) v hodnote 240 000 Eur a administratívne náklady 10 000 Eur.
- V Roku 2 predpokladáme investičné náklady v hodnote 794 639 Eur, ktoré zahŕňajú interné náklady na personálne zabezpečenie v hodnote 205 324 Eur a externé náklady na implementáciu 589 315 Eur.

- V ďalších 5-ich rokoch tzn. Rok 3 až Rok 7 sú ročné predpokladané náklady 621 210 Eur, ktoré zahŕňajú interné náklady na personálne zabezpečenie vo výške 326 408 Eur, iné podporné externé služby 240 000 Eur ako aj ďalšie náklady na prevádzku systému a administratívne náklady.

V interných nákladoch pre Rok 1 a 2 sú zahrnuté nasledujúce predpokladané náklady na interných pracovníkov pre prípravu a implementáciu sandboxu v sume 205 324 Eur ročne¹¹¹:

- 1x vedúci sandboxu: 48 600 Eur ¹¹²
- 1x odborník na reguláciu: 34 020 Eur ¹¹³
- 1x špecialista na umelú inteligenciu a technológie: 56 700 Eur ¹¹⁴
- 1x podporný personál: projektový manažér: 35 640 Eur ¹¹⁵
- 1x podporný personál: administratívny pracovník: 30 364 Eur¹¹⁶

Po nastavení organizácie sandboxu a implementácie technickej podpory predpokladáme navýšenie počtu interných pracovníkov s ročnými nákladmi 326 408 Eur:

- 1x vedúci sandboxu: 48 600 Eur
- 2x odborník na reguláciu: 68 040 Eur
- 2x špecialista na umelú inteligenciu a technológie: 113 400 Eur
- 1x podporný personál: projektový manažér: 35 640 Eur
- 2x podporný personál: administratívny pracovník: 60 728 Eur

Celkové predpokladané trvanie vytvorenia všetkých súčastí sandboxu je 24 mesiacov (vrátane prípravy legislatívy, organizácie a implementácie IT riešenia) s následnou 1 mesačnou stabilizačnou aktivitou.

¹¹¹ Poznámka: Zdroje k odhadovanému výpočtu nákladov vychádzajú z verejne dostupných údajov o hrubej mzde, ktorá je zvýšená o zaokrúhlený koeficient 35% z dôvodu zahrnutia nákladov na strane zamestnávateľa.

¹¹² Zdroj odhadu: https://www.profesia.sk/praca/ministerstvo-investicii-regionalneho-rozvoja-a-informatizacie-slovenskej-republiky/O4665112?search_id=cbcc9c2b-d637-4f1e-89f6-c56508d6d3ad

¹¹³ Zdroj odhadu: https://www.profesia.sk/praca/tatra-banka/O4721389?search_id=4860078b-a3c2-43e1-b1c2-c4c0d159be7e

¹¹⁴ Zdroj odhadu: https://www.profesia.sk/praca/dell-technologies/O4716669?search_id=608f6b08-c886-4ae7-8ced-a63d84ae75c1

¹¹⁵ Zdroj odhadu: <https://mirri.gov.sk/kariera/kariera-u-nas/archiv-ukoncene-vyberove-konania/projektovy-manazer-pre-digitalne-inovacie/>

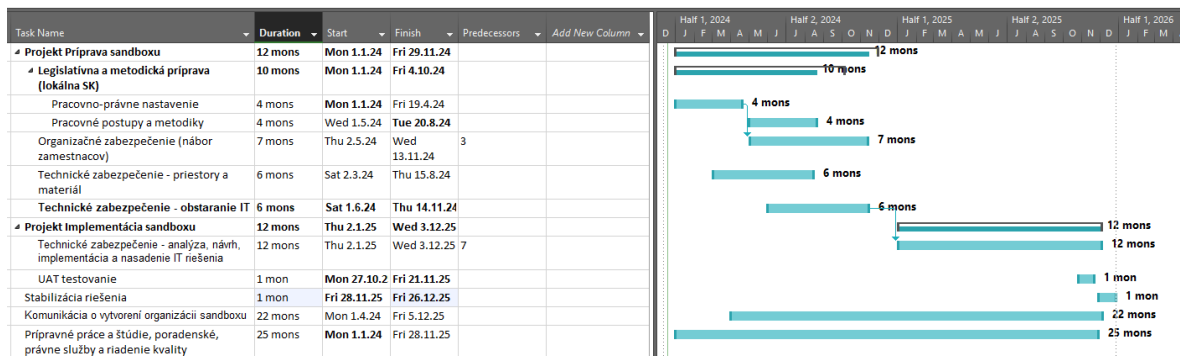
¹¹⁶ Zdroj odhadu: Štatistický úrad SR. Priemer 1. až 3. kvartálu v roku 2023 v sektore Verejná správa a obrana: https://datacube.statistics.sk/#/view/sk/VBD_INTERN/pr0205qs/v_pr0205qs_00_00_00_sk

Tabuľka č.24.: Predpokladané aktivity a trvanie implementácie a prevádzky

	Oblasť implementácie	Aktivity	Navrhovaný projekt	Predpokladané trvanie v mesiacoch (trvanie aktivít sa predpokladá z časti paralelne)	Zodpovední
1	Legislatívna a metodická príprava	- Legislatívne úpravy - Inštitucionálne zakotvenie sandboxu, vrátane alokácie kompetencií OVM SR - Vykonávacia a metodická dokumentácia k organizačnému a procesnému zabezpečeniu fungovania sandboxu	Projekt Príprava sandboxu	7	Príslušné OVM a zriaďujúci orgán Pozn. pri zohľadnení záverov a odporúčaní TSI Analýzy (v relevantnom rozsah)
2	Organizačné zabezpečenie	- Vytvorenie popisu pracovných pozícií a pracovných miest - Nábor zamestnancov		7	Zriaďujúci orgán
3	Technické zabezpečenie - priestory a materiál	Vytvorenie priestorového a materiálneho zabezpečenia (kancelárie, zariadenie)		6	Zriaďujúci orgán
4	Technické zabezpečenie - obstaranie IT	Vytvorenie zadávacej dokumentácie pre obstarávanie IT riešenia a poradenských prác		6	Zriaďujúci orgán
5	Technické zabezpečenie - implementácia IT	- Technické zabezpečenie - analýza, návrh, implementácia a nasadenie IT riešenia - Testovanie a nasadenie riešenia	Projekt Implementácia sandboxu	12	Zriaďujúci orgán a externý dodávateľ
6	Komunikácia o vytvorení organizácii sandboxu	- Vytvorenie komunikačnej stratégie - Vytvorenie webového sídla - Zverejnenie materiálov pre	Projekt Príprava sandboxu/Projekt Implementácia sandboxu	22	Zriaďujúci orgán

	Oblasť implementácie	Aktivity	Navrhovaný projekt	Predpokladané trvanie v mesiacoch (trvanie aktivít sa predpokladá z časti paralelne)	Zodpovední
		verejnosť			
7	Prípravné práce a štúdie, poradenské, právne služby a riadenie kvality	Podporné činnosti pre prípravu, napr. metodické a pracovné postupy, konzultácie v oblasti umelej inteligencie, správy a ochrany dát a pod.	Projekt Príprava sandboxu/Projekt Implementácia sandboxu	25	Zriaďujúci orgán
8	Stabilizácia riešenia	Stabilizácia a monitorovanie riešenia po jeho uvedení do živej prevádzky	Projekt implementácia	1	Zriaďujúci orgán
9	Prevádzka	Prevádzka po ukončení projektov (predpoklad 5 rokov)	Prevádzka	60	Zriaďujúci orgán

Obrázok č.8.: Predpokladaný časový rámec implementácie



5.8 Cestovná mapa implementácie a Návrh postupu implementácie regulačného experimentálneho prostredia

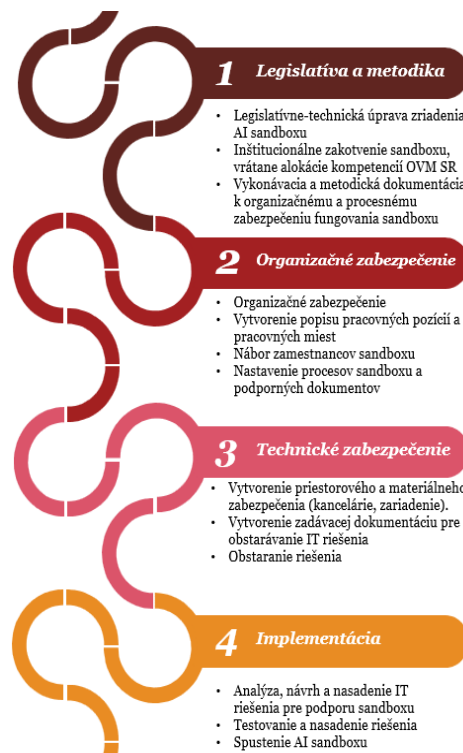
Cestovná mapa implementácie predstavuje znázornenie základných krokov, ktoré sú potrebné pre zriadenie “ekosystému” AI sandboxu od legislatívneho a metodického ukotvenia, cez organizačné zabezpečenie až po implementáciu technického riešenia.

Cestovnú mapu je možné rozdeliť do 2 základných projektov a to:

1. **Projekt Príprava sandboxu** (zahŕňa oblasti 1. legislatívna a metodika, 2. organizačné zabezpečenie, 3. technické zabezpečenie)
2. **Projekt Implementácia sandboxu** zahŕňa oblasť: 4. (implementácia a nasadenie IT riešenia)

Významnou aktivitou, ktorá by mala prebiehať paralelne od začiatku do konca realizácie AI sandboxu bude nastavenie komunikačnej stratégie smerom k potenciálnym uchádzačom a odbornej verejnosti, pre vytvorenie čo najjednoduchšieho prístupu a využitia AI sandboxu.

Obrázok č. 9: Cestovná mapa implementácie AI sandboxu



6 Limitácie

- Požiadavky na zriaďovanie a fungovanie AI sandboxov v zmysle Nariadenia sa môžu ďalej meniť aj v závislosti od úprav textu Nariadenia v legislatívnom procese a obsahu delegovaných aktov Komisie, ktoré majú ba budúce nastavenie vzťahov k sandboxu bude musieť zohľadňovať aktualizované znenie.
- V prípade, ak Štúdia odkazuje na právne predpisy, ktoré boli v čase prípravy Štúdie ešte v legislatívnom procese, je potrebné upozorniť na to, že znenia daných predpisov sa môžu ďalej meniť (okrem iného aj v závislosti od finalizácie textu Nariadenia) a budúce nastavenie vzťahov k sandboxu pre umelú inteligenciu v prostredí SR bude musieť zohľadňovať právnu úpravu vyplývajúcu z ich finálneho znenia)).
- Nevykonali sme nič, čo by svojou podstatou pripomínalo audit, a s výnimkou prípadov, kde je uvedené inak, sme finančné či iné informácie obsiahnuté v tejto správe ani nekontrolovali a ani neoverovali. V súlade s tým (okrem prípadov, kde je uvedené inak) preto nepreberáme nijakú zodpovednosť za správnosť, presnosť či úplnosť informácií uvedených v tejto správe a nedávame v tomto smere ani nijaké vyhlásenia.
- Kvôli obmedzenému rozsahu našich prác a z dôvodu, že postupy nemajú svojím charakterom predstavovať audit, preverenie či nejakú inú formu uisťovacej zákazky realizovanej v súlade s platnými štandardmi pre audit, preverovanie či iné uisťovacie služby, nevyslovujeme nijaký typ uistenia ohľadom Štúdie realizovateľnosti vo forme vyjadrenia nejakého názoru či celkového záveru.
- Spoločnosť PwC nie je zodpovedná za posúdenie dostatočnosti postupov špecifikovaných v tejto správe či už pre účel, pre ktorý boli tieto postupy vyžiadané, alebo pre nejaký iný účel.
- Z vyššie uvedených dôvodov sa môže stať, že táto správa nemusí nutne odhaliť všetky problematické oblasti, ktoré by Vás mohli zaujímať.
- Ak by sme boli vykonali ďalšie postupy príp. ak by sme boli realizovali audit, preverenie či nejaké iné uisťovacie postupy v súlade s platnými štandardmi pre audit, preverovanie či iné uisťovacie služby, možno by sme boli narazili aj na iné veci, o ktorých by sme Vás ihneď informovali.
- Kontrolné mechanizmy a postupy na riadenie rizík už svojou podstatou nemôžu zabrániť či odhaliť a napraviť všetky chyby či opomenutia. Takisto projekcia do budúcnosti ohľadom vyhodnotenia vhodnosti formy či prevádzkovej efektívnosti kontrolných mechanizmov naráža na riziko, že sa kontrolné mechanizmy a postupy na riadenie rizík nebudú javiť ako dostatočné alebo že dokonca zlyhajú.
- Kópie tejto správy nesmiete poskytnúť žiadnym iným stranám okrem tých, ktoré sú uvedené v objednávke zo dňa 9.11.2023. Nepreberáme preto na seba povinnosť starostlivosti (či už na základe zmluvy, prečinu (vrátane prečinu z nedbalosti) či iného dôvodu) voči akejkoľvek osobe inej než Vašej, pokiaľ nie je v zmluve dojednané niečo iné.



Ak by ste mali nejaké otázky či už ohľadom správy samotnej alebo ohľadom zistení, ktoré obsahuje, obráťte sa prosím bez váhania na [meno a priezvisko, e-mailová adresa, telefónne číslo.]

PricewaterhouseCoopers Slovensko, s.r.o.

Bratislava

15.12.2023