SBA
SLOVAK | BUSINESS | AGENCY

DOPADY TECHNOLOGICKÝCH REGULÁCIÍ EÚ NA KONKURENCIESCHOPNOSŤ MSP NA SLOVENSKU

BRATISLAVA
2026

Vydavateľ:

Slovak Business Agency

Neprešlo jazykovou úpravou.

OBSAH

Zoznam tabuliek

Zoznam skratiek

Akt o kybernetickej odolnosti (CRA) alebo CR	Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)
BigTech	veľké technologické spoločnosti
CAGR	zložená ročná miera rastu
CEPR	Centre for Economic Policy Research
CEPS	Centre for European Policy Studies
CINECA	Talianske výskumné centrum pre vysokovýkonné počítanie, veľké dáta a kvantové počítanie
CISO	Cybersecurity officer / riadiaci pracovník zodpovedný za implementáciu a dohľad nad kybernetickou bezpečnosťou
DESI	Index digitálnej ekonomiky a spoločnosti
EDIH	European Digital Innovation Hubs / Európske centrá digitálnych inovácií
EHP	Európsky hospodársky priestor
ENISA	Agentúra Európskej únie pre kybernetickú bezpečnosť
EUSAiR	EU Regulatory Sandboxes for AI
EÚ	Európska únia
GDPR	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)
IoT	Internet of Things
MIRRI	Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky

MSP	malé a stredné podniky
Nariadenie o umelej inteligencii (AI Act) alebo AI Act	Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES) č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii)
NBÚ SR	Národný bezpečnostný úrad Slovenskej republiky
QMS	Quality Management System
Registr PZS	register prevádzkovateľov základných služieb
SAFE	Survey on the Access to Finance of Enterprises
SBOM	**Software Bill of Materials**
Smernica NIS2 alebo **NIS2**	Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)
SOI	Slovenská obchodná inšpekcia
SR	Slovenská republika
TEFs	Testing and Experimentation Facilities / zariadenia pre testovanie a experimentovanie
UNCTAD	United Nations Conference on Trade and Development / Konferencia Spojených národov pre obchod a rozvoj
Zákon o kybernetickej bezpečnosti	zákon č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov

Manažérske zhrnutie

Analýza hodnotí dopady troch kľúčových technologických regulácií Európskej únie na malé a stredné podniky (MSP) na Slovensku: AI Act, Cyber Resilience Act (CRA) a NIS2. Primárny záver vyplývajúci z tejto analýzy je, že tieto regulácie predstavujú pre slovenské MSP citeľnú zmenu podnikateľského prostredia, ktorá zároveň prináša zvýšené náklady, nové povinnosti, ale aj nové trhové príležitosti.

MSP tvoria rozhodujúcu časť slovenskej ekonomiky, a preto akékoľvek systematické zvýšenie regulačných nárokov bude mať priamy dopad na konkurencieschopnosť Slovenska ako celku. Technologické regulácie EÚ sa pritom netýkajú iba úzko definovaného IT sektora. Ich dosah je širší. Zasahujú výrobcov digitálnych produktov, podniky využívajúce AI, subjekty pôsobiace v regulovaných sektoroch podľa NIS2, ale aj mnohé firmy nepriamo cez dodávateľské reťazce.

Podstatným záverom tejto analýzy je zistenie, že AI Act, CRA a NIS2 majú merateľný nákladový dopad, pričom menšie podniky budú túto záťaž znášať ťažšie ako väčšie firmy. Analýza zároveň vychádza zo skúseností s GDPR a konštatuje, že pri malých podnikoch a mikropodnikoch možno očakávať náklady na compliance v rozsahu približne 0,8 až 1,9 % z obratu. Ide o úroveň, ktorá už môže citeľne konkurovať výdavkom na rozvoj, inovácie alebo výskum, a teda náklady, ktoré prináša nová regulácia, môžu odčerpávať zdroje, ktoré by inak smerovali do rastu a inovácií.

Na druhej strane analýza upriamuje pozornosť aj na tú skutočnosť, že compliance a súlad MSP s AI Act, CRA a NIS2, môže priniesť aj konkrétne obchodné benefity. Napríklad jednoduchší prístup na jednotný trh EÚ, vyššiu dôveru zákazníkov a partnerov, nižšie riziko bezpečnostných incidentov, lepšiu pozíciu v dodávateľských reťazcoch a možnosť využiť vysokú imeru európskych štandardov pri expanzii na ďalšie trhy. Inak povedané, podnik, ktorý bude vedieť preukázať bezpečnosť, transparentnosť a zodpovedný prístup, môže získať konkurenčnú výhodu.

Regulačnými povinnosťami budú dotknuté najmä tieto skupiny podnikov:

- poskytovatelia vysokorizikových AI systémov,
- výrobcovia IoT zariadení a softvérových produktov,
- podniky v sektoroch regulovaných NIS2, ako energetika, doprava, zdravotníctvo či digitálna infraštruktúra,
- dodávatelia kritických komponentov alebo služieb väčším regulovaným subjektom, na ktorých sa požiadavky prenesú nepriamo.

Naopak, regulačnými povinnosťami menej zasiahnuté budú mikropodniky a malé podniky mimo regulovaných sektorov, tradičné služby bez výraznej digitálnej zložky a podniky fungujúce výlučne lokálne. Aj tieto podniky sa však budú musieť v niektkrých prípadoch regulácii prispôsobiť, nakoľko požiadavky na ne môžu preniesť iné, viac regulované subjekty (cez zákazníkov či verejné obstarávanie).

Analýza identifikuje viacero systémových rizík, ktoré sa môžu dotknú MSP. Patria sem zvýšené náklady, ktoré sa vzhľadom na nižší rozpočet MSP v porovnaní s veľkými podnikmi môžu javiť ako neúmerne vysoké. Ďalším rizikom je nedostatok kvalifikovaných odborníkov,

najmä v oblastiach kybernetickej bezpečnosti, AI a compliance na trhu. Tretím rizikom je regulačná neistota, spôsobená postupným vydávaním ďalších usmernení a výkladov regulačných aktov AI Act, CRA a NIS2. Štvrtým rizikom je, že slovenské MSP nevyužijú existujúce podporné mechanizmy a tým si samy znížia šancu efektívne zvládnuť prechod na nové podmienky.

Z praktického hľadiska možno MSP odporučiť nasledovné kroky:

Prvým krokom je sumarizácia, aké AI nástroje konrétny podnik používa, aké digitálne produkty vyrába alebo predáva a či patrí do okruhu subjektov pod NIS2. Pri AI Acte je dôležité odlíšiť, či je firma len používateľom AI, alebo aj poskytovateľom AI systému. Pri CRA je kľúčové vedieť, či firma uvádza na trh produkty s digitálnymi prvkami (products with digital elements). Pri NIS2 treba overiť, či podnik pôsobí v regulovanom sektore alebo je kritickým dodávateľom pre subjekt, na ktorý sa NIS2 vzťahuje.

Pri AI Act je prvoradé zvýšiť AI gramotnosť vo firme. Článok 4 AI Actu vyžaduje, aby poskytovatelia a používatelia AI prijali opatrenia na zabezpečenie dostatočnej úrovne AI gramotnosti osôb, ktoré AI používajú alebo prevádzkujú v ich mene. Regulácia a compliance by nemala byť len „na papieri“, pretože si objektívne vyžaduje optimalizáciu firemných procesov. Na mieste je preto zaviesť interné pravidlá, na čo sa AI smie a nesmie používať a najmä kto vo firme bude AI nástroje využívať. Rozhodne je vhodné zaviesť povinnosť ľudskej kontroly výstupov AI pri HR, zmluvách, zákazníckej komunikácii a rozhodovaní s právnym alebo faktickým dopadom.

CRA sa netýka každej firmy, ale ak MSP vyrába alebo dodáva softvér, aplikáciu, firmware, IoT zariadenie alebo iný digitálny produkt, regulácia na podnik resp. dopad naň môže byť zásadný. Komisia pri výklade pre výrobcov uvádza, že prvým krokom je risk assessment, na základe ktorého sa určujú primerané základné požiadavky kybernetickej bezpečnosti. Následne treba tieto požiadavky vysvetliť v technickej dokumentácii a vykonať conformity assessment. CRA tiež vyžaduje, aby boli produkty navrhnuté, aktualizované a udržiavané počas životného cyklu. Reportingové povinnosti sa začnú uplatňovať od 11. septembra 2026 a plná aplikácia CRA od 11. decembra 2027.

Ak firma spadá pod NIS2 alebo je významným dodávateľom subjektu pod NIS2, je potrebné v prvom rade zvážiť prijatie **primeraných technické, prevádzkových a organizačných opatrení, pričom** ENISA poskytuje pomerne praktické a zrozumiteľné usmernenia. Samotná smernica kladie dôraz na autorizáciu prijatých opatrení vedením, dohľad nad ich implementáciou a pravidelné školenie manažmentu a zamestnancov.

Najefektívnejší postup pre MSP je **neriešiť compliance vo vzťahu k AI Act, CRA a NIS2 izolovane (oddelene)**, ale vo vzájomných súvislostiach cez jeden spoločný risk-management proces. Všetky tri regulačné rámce totiž vo svoje podstate riešia podobné otázky: aké systémy podnik používa, aké riziká pri tom vznikajú, kto za ne zodpovedá, aké opatrenia už má podnik prijaté, ako ich prijatie preukázať a ako postupovať pri incidente. AI Act výslovne pracuje s rizikovým prístupom, CRA začína risk assessmentom a NIS2 vyžaduje cybersecurity risk-management measures.

Dôležité je tiež neopomenúť úlohu štátu. Úspešná implementácia technologických regulácií si vyžaduje koordinovaný systém podpory v piatich oblastiach: metodická

a informačná podpora, finančné nástroje, legislatívna a regulačná podpora, vzdelávanie a budovanie kapacít a podpora networkingu, zdieľaných služieb a exportu. K prioritám možno zaradiť spustenie jednotného informačného portálu, rozšírenie grantovej schémy na kybernetickú bezpečnosť, zriadenie regulačného sandboxu pre AI do augusta 2026, rozšírenie kapacít EDIH na AI helpdesk a programy AI gramotnosti.

1 ÚVOD

1.1 Kontext technologických regulácií a význam pre MSP

Európska únia v posledných rokoch výrazne zintenzívnila svoje úsilie v oblasti regulácie digitálnych technológií. Tento trend je odpoveďou na dynamický technologický vývoj, rastúce kybernetické hrozby a potrebu zabezpečiť, aby nové technológie – najmä umelá inteligencia a pripojené zariadenia – boli bezpečné, etické a rešpektovali základné práva občanov. Pre malé a stredné podniky (MSP) predstavujú tieto regulácie zásadnú zmenu podnikateľského prostredia, ktorá si vyžaduje systematickú prípravu a investície do compliance.

Postavenie MSP v európskej a slovenskej ekonomike

MSP tvoria základný pilier európskej ekonomiky. Podľa údajov Eurostatu z roku 2022 bolo v Európskej únii aktívnych 32,3 milióna podnikov, z ktorých 99 % tvorili mikropodniky a malé podniky zamestnávajúce do 49 osôb[1]. Tieto podniky zamestnávali 77,5 milióna osôb, čo predstavuje takmer polovicu (48 %) celkovej zamestnanosti v podnikovej ekonomike. Stredné podniky (50-249 zamestnancov) tvorili ďalších 0,8 % všetkých podnikov a podieľali sa na 15 % zamestnanosti. Spoločne tak mikropodniky a MSP predstavujú 99,8 % všetkých podnikov v EÚ a poskytujú prácu viac ako 85 miliónom európskych občanov.

Na Slovensku je situácia obdobná. Podľa Správy o stave MSP na Slovensku za rok 2024[2], ktorú pripravuje Slovak Business Agency, MSP dosiahli 99,9 % podiel na celkovom počte ekonomicky aktívnych podnikateľských subjektov. V absolútnych číslach to v roku 2024 predstavovalo 683 937 malých a stredných podnikateľov (mierny nárast oproti predchádzajúcemu roku, keď ich bolo o 16 999 menej). Podiel MSP na zamestnanosti v podnikovej ekonomike dosiahol 74,9 % a na celkovej zamestnanosti v hospodárstve SR 59,1 %. Tieto čísla jednoznačne potvrdzujú, že konkurencieschopnosť a adaptabilita MSP priamo ovplyvňujú celkovú výkonnosť slovenskej ekonomiky.

Digitálna transformácia a jej výzvy pre Slovensko

Digitálna transformácia je jednou z kľúčových priorít Európskej únie pre obdobie 2019-2024. Európska komisia monitoruje digitálny pokrok členských štátov prostredníctvom Indexu digitálnej ekonomiky a spoločnosti (DESI). Slovensko sa v tomto hodnotení dlhodobo umiestňuje v poslednej tretine rebríčka členských štátov EÚ. V roku 2023 mala úroveň základných digitálnych zručností na Slovensku hodnotu 51 %, čo je pod priemerom EÚ (55 %)[3]. Prieskumy tiež ukazujú, že viac ako 44 % slovenských podnikov považuje nedostatok digitálnych zručností svojich zamestnancov za významnú prekážku pre úspešnú implementáciu digitálnych technológií.

[1] https://www.teraz.sk/ekonomika/minuly-rok-malo-v-eu-335-miliona-pod/926631-clanok.html
[2] https://www.npc.sk/media/final_final_sprava_o_stave_MSP_2024_kom_LLtm-zps.pdf
[3] https://digitalnabuducnost.gov.sk/digitalne-zrucnosti-na-slovensku-najaktualnejsie-data-ukazuju-kde-napredujeme-a-kde-zaostavame/

Stratégia digitálnej transformácie Slovenska 2030 definuje cieľ, aby sa Slovensko stalo modernou krajinou s inovačným a ekologickým priemyslom, efektívnou verejnou správou a informačnou spoločnosťou, ktorej občania budú naplno využívať svoj potenciál v digitálnej dobe. Hlavným cieľom stratégie na zlepšenie postavenia Slovenska v indexe DESI do roku 2025 je posunúť krajinu z poslednej tretiny rebríčka do jeho stredu a dosiahnuť aspoň priemer EÚ. V tomto kontexte predstavujú nové technologické regulácie EÚ dvojsečnú výzvu – na jednej strane zvyšujú administratívnu a finančnú záťaž, na druhej strane môžu byť katalyzátorom modernizácie a zvýšenia dôveryhodnosti slovenských podnikov na európskom trhu.

Tri kľúčové technologické regulácie EÚ

Táto analýza sa zameriava na tri kľúčové regulačné rámce, ktoré budú mať zásadný vplyv na podnikanie MSP v najbližších rokoch:

Nariadenie o umelej inteligencii (AI Act) – Nariadenie (EÚ) 2024/1689 predstavuje prvý komplexný právny rámec pre umelú inteligenciu na svete. Nadobudlo účinnosť 1. augusta 2024 a bude plne aplikovateľné od 2. augusta 2026. Regulácia zavádza prístup založený na rizikách, ktorý kategorizuje AI systémy do štyroch úrovní: minimálne riziko, obmedzené riziko, vysoké riziko a neprijateľné riziko. Pre MSP je kľúčové, že nariadenie obsahuje osobitné ustanovenia na ich podporu, vrátane zjednodušenej technickej dokumentácie a prioritného prístupu do regulačných sandboxov.

Akt o kybernetickej odolnosti (CRA) – Nariadenie (EÚ) 2024/2847 nadobudlo účinnosť 10. decembra 2024, pričom hlavné povinnosti sa budú uplatňovať od 11. decembra 2027. CRA zavádza horizontálne požiadavky na kybernetickú bezpečnosť pre všetky produkty s digitálnymi prvkami uvádzané na trh EÚ. Výrobcovia budú musieť zabezpečiť, aby ich produkty boli navrhnuté, vyvinuté a vyrobené v súlade so základnými požiadavkami na kybernetickú bezpečnosť, vrátane princípov 'security by design' a 'security by default'. Povinnosť hlásiť zraniteľnosti a incidenty agentúre ENISA do 24 hodín nadobúda účinnosť už od 11. septembra 2026.

Smernica NIS2 – Smernica (EÚ) 2022/2555 bola prijatá v decembri 2022 s cieľom posilniť kybernetickú bezpečnosť kritických sektorov v celej EÚ. Na Slovensku bola transponovaná novelou zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti (zákon č. 366/2024 Z. z.), ktorá nadobudla účinnosť 1. januára 2025. Podľa dôvodovej správy sa novela dotýka minimálne 3 403 organizácií na Slovensku a upravuje viac ako 80 služieb v 16 odvetviach. Smernica sa primárne vzťahuje na stredné a veľké podniky v regulovaných sektoroch, avšak nepriamo ovplyvňuje aj menšie podniky prostredníctvom požiadaviek na bezpečnosť dodávateľského reťazca.

Ciele tejto analýzy

Hlavným cieľom tejto analýzy je komplexne zhodnotiť dopady uvedených troch technologických regulácií EÚ na konkurencieschopnosť MSP na Slovensku. Analýza si kladie za cieľ:

- Identifikovať priame a nepriame náklady, ktoré budú musieť MSP vynaložiť na dosiahnutie súladu s novými reguláciami.

- Identifikovať najzraniteľnejšie segmenty MSP z hľadiska pripravenosti na nové požiadavky.
- Zhodnotiť stav transpozície a implementácie regulácií do slovenského právneho poriadku.
- Navrhnúť konkrétne odporúčania pre metodickú, finančnú a legislatívnu podporu zo strany štátu.
- Poskytnúť praktické odporúčania pre samotné MSP na úspešné zvládnutie regulačných zmien.

Výstupom analýzy bude komplexné zhodnotenie, ktoré umožní tvorcom politík, podnikateľským združeniam aj samotným MSP lepšie pochopiť rozsah a charakter nadchádzajúcich zmien a pripraviť sa na ne strategicky a efektívne.

1.2 Vymedzenie pojmov a definície MSP

Pre správne pochopenie problematiky a konzistentné používanie terminológie v celej analýze je nevyhnutné jasne vymedziť kľúčové pojmy a definície, s ktorými pracujú analyzované právne normy.

Definícia malých a stredných podnikov podľa EÚ

Základným referenčným dokumentom pre definíciu MSP v Európskej únii je Odporúčanie Komisie 2003/361/ES zo 6. mája 2003, ktoré nadobudlo účinnosť 1. januára 2005. Podľa tohto odporúčania sa kategória MSP skladá z podnikov, ktoré zamestnávajú menej ako 250 osôb a ktorých ročný obrat nepresahuje 50 miliónov EUR a/alebo celková ročná bilančná suma nepresahuje 43 miliónov EUR. Táto definícia je záväzná pre účely štátnej pomoci, štrukturálnych fondov a ďalších programov EÚ.

V rámci kategórie MSP sa rozlišujú tri podkategórie:

- **Mikropodnik** – podnik, ktorý zamestnáva menej ako 10 osôb a ktorého ročný obrat a/alebo celková ročná bilančná suma nepresahuje 2 milióny EUR.
- **Malý podnik** – podnik, ktorý zamestnáva menej ako 50 osôb a ktorého ročný obrat a/alebo celková ročná bilančná suma nepresahuje 10 miliónov EUR.
- **Stredný podnik** – podnik, ktorý zamestnáva menej ako 250 osôb a ktorého ročný obrat nepresahuje 50 miliónov EUR alebo celková ročná bilančná suma nepresahuje 43 miliónov EUR.

Pri posudzovaní, či podnik spadá do kategórie MSP, je potrebné zohľadniť aj vzťahy s partnerskými a prepojenými podnikmi. Autonómny podnik je taký, ktorý nie je partnerským ani prepojeným podnikom. Ak podnik vlastní 25 % alebo viac kapitálu alebo hlasovacích práv iného podniku, alebo ak iný podnik vlastní takýto podiel v danom podniku, je potrebné údaje o zamestnancoch a finančných ukazovateľoch konsolidovať.

Definície relevantné pre AI Act

Nariadenie o umelej inteligencii pracuje s niekoľkými kľúčovými pojmami:

- **Systém umelej inteligencie (AI systém)** – strojový systém navrhnutý na prevádzku s rôznou úrovňou autonómie, ktorý môže po nasadení vykazovať adaptabilitu a ktorý

pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré prijíma, ako generovať výstupy.
- **Poskytovateľ (provider)** – fyzická alebo právnická osoba, ktorá vyvíja AI systém alebo model všeobecného účelu alebo dá vyvinúť AI systém či model a uvádza ho na trh alebo do prevádzky pod vlastným menom alebo ochrannou známkou.
- **Nasadzovateľ (deployer)** – fyzická alebo právnická osoba, ktorá používa AI systém pod vlastnou právomocou, s výnimkou osobného nekomerčného použitia.
- **Vysokorizikový AI systém** – AI systém, ktorý spadá do jednej z kategórií uvedených v prílohe III nariadenia a ktorý predstavuje významné riziko pre zdravie, bezpečnosť alebo základné práva fyzických osôb.
- **Regulačný sandbox** – kontrolované prostredie zriadené príslušným orgánom, ktoré umožňuje vývoj, testovanie a validáciu AI systémov pred ich uvedením na trh podľa špecifického plánu pod dohľadom regulátora.

Definície relevantné pre Cyber Resilience Act

Akt o kybernetickej odolnosti definuje nasledujúce kľúčové pojmy:
- **Produkt s digitálnymi prvkami –** akýkoľvek softvérový alebo hardvérový produkt a jeho riešenia na spracovanie údajov na diaľku, vrátane softvérových alebo hardvérových komponentov, ktoré sa uvádzajú na trh samostatne, ak ich zamýšľané alebo rozumne predvídateľné použitie zahŕňa priame alebo nepriame logické alebo fyzické dátové spojenie so zariadením alebo sieťou.
- **Výrobca** – fyzická alebo právnická osoba, ktorá vyrába produkt s digitálnymi prvkami alebo dá takýto produkt navrhnúť alebo vyrobiť a uvádza ho na trh pod svojím menom alebo ochrannou známkou.
- **Dovozca** – fyzická alebo právnická osoba usadená v Únii, ktorá uvádza na trh Únie produkt s digitálnymi prvkami nesúci meno alebo ochrannú známku fyzickej alebo právnickej osoby usadenej mimo Únie.
- **Distribútor** – fyzická alebo právnická osoba v dodávateľskom reťazci, iná ako výrobca alebo dovozca, ktorá sprístupňuje produkt s digitálnymi prvkami na trhu Únie.
- **Aktívne zneužívaná zraniteľnosť** – zraniteľnosť, o ktorej existujú spoľahlivé dôkazy, že ju škodlivý aktér zneužil v systéme bez povolenia vlastníka systému.

Definície relevantné pre NIS2 a slovenský zákon o kybernetickej bezpečnosti

Smernica NIS2 a jej slovenská transpozícia pracujú s nasledujúcimi pojmami:
- **Prevádzkovateľ základnej služby** – verejný alebo súkromný subjekt, ktorý poskytuje službu kritickú pre fungovanie spoločnosti a hospodárstva v niektorom z regulovaných sektorov a spĺňa veľkostné kritériá (spravidla stredný alebo veľký podnik).
- **Kľúčový subjekt** – subjekt uvedený v prílohe I smernice (sektory s vysokou úrovňou kritickosti), ktorý presahuje limity pre stredné podniky alebo je identifikovaný ako kritický bez ohľadu na veľkosť.
- **Dôležitý subjekt** – subjekt uvedený v prílohe II smernice (iné kritické sektory), ktorý spĺňa veľkostné kritériá pre stredný podnik.
- **Kybernetický bezpečnostný incident** – udalosť ohrozujúca dostupnosť, autentickosť, integritu alebo dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo služieb ponúkaných alebo prístupných prostredníctvom sietí a informačných systémov.

- **Bezpečnostné opatrenia** – primerané a proporcionálne technické, prevádzkové a organizačné opatrenia na riadenie rizík ohrozujúcich bezpečnosť sietí a informačných systémov.

Prepojenie regulácií a ich vzájomné vzťahy

Je dôležité si uvedomiť, že analyzované regulácie sa vzájomne dopĺňajú a v niektorých prípadoch prekrývajú. AI Act výslovne stanovuje, že ak produkt spĺňa požiadavky na kybernetickú bezpečnosť podľa CRA, považujú sa za splnené aj príslušné požiadavky podľa AI Act (článok 12 CRA). Podobne, podniky spadajúce pod NIS2 budú musieť zabezpečiť kybernetickú bezpečnosť celého dodávateľského reťazca, čo vytvorí tlak aj na menších dodávateľov, ktorí síce priamo pod NIS2 nespadajú, ale budú musieť preukazovať úroveň svojej kybernetickej odolnosti. Pochopenie týchto prepojení je kľúčové pre efektívne plánovanie compliance aktivít a optimalizáciu nákladov.

2 LEGISLATÍVNY RÁMEC

V tejto kapitole vysvetlíme podstatu regulácie jednotlivých právnych aktov a detailne vymedzíme, koho (ktorých subjektov) sa ten-ktorý akt týka a čo primárne upravuje.

Osobitná podkapitola sa zameria na stav transpozície a implementácie do právneho poriadku SR, ktoré povinnosti už boli premietnuté do slovenského právneho poriadku a aké legislatívne zmeny sa ešte pripravujú.

2.1 Nariadenie (EÚ) 2024/1689 – AI Act

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/1689 z 13. júna 2024, ktorým sa stanovujú harmonizované pravidlá v oblasti umelej inteligencie a ktorým sa menia nariadenia (ES)m č. 300/2008, (EÚ) č. 167/2013, (EÚ) č. 168/2013, (EÚ) 2018/858, (EÚ) 2018/1139 a (EÚ) 2019/2144 a smernice 2014/90/EÚ, (EÚ) 2016/797 a (EÚ) 2020/1828 (akt o umelej inteligencii) (Text s významom pre EHP z 13. júna 2024, je úplný názov tohto nariadenia o regulácii umelej inteligencie. Toto nariadenie sa skrátene označuje aj ako Akt o umelej inteligencii alebo AI Act.

Akt o umelej inteligencii je právnou normou, ktorá reguluje vývoj a vplyv významných technológií na spoločnosť. Cieľom Aktu o umelej inteligencii bolo vytvoriť regulačný rámec, ktorý by chránil základné práva a demokratické hodnoty, vytvoril záruky pre bezpečné systémy umelej inteligencie, chránil používateľov pred rizikami spojenými s umelou inteligenciou a podporoval inovácie a konkurencieschopnosť EÚ v tejto technologickej oblasti.

Akt o umelej inteligencii je právnou reguláciou, ktorá si stanovila za cieľ dosiahnuť rovnováhu medzi reguláciou a rozvojom umelej inteligencie.

2.1.1 Účel AI Act

Účelom prijatia tejto regulácie bolo vytvorenie právne záväzných pravidiel, ktoré majú zabezpečiť budúci vývoj AI technológií tak, aby sa kontrolovali riziká spojené s používaním a vývojom určitých typov modelov.

Prvým krokom k dosiahnutiu tohto cieľa nariadenia je vymedzenie zodpovedností subjektov v rámci životného cyklu hodnotového reťazca umelej inteligencie. Medzi tieto subjekty patria vývojári, distribútori, koneční používatelia a ďalší. Druhým bodom je stanovenie požiadaviek na transparentnosť, bezpečnosť a zodpovednosť. Modely musia spĺňať tieto požiadavky počas celého svojho životného cyklu, od uvedenia na trh až po ukončenie podpory.

2.1.2 Ciele AI Act

AI Act si stanovuje viacero cieľov, ktoré sú vzájomne prepojené.

- **Ochrana základných práv a slobôd a ochrana bezpečnosti** – najmä ochrana súkromia a bezpečnosti a zákaz nebezpečných a neetických systémov, ako napr. tzv. „social scoring“ – hodnotenie osôb na základe rôznych ekonomických

a sociálnych aspektov. Akt tiež stanovuje potrebu kontroly nad modelmi umelej inteligencie, aby nedochádzalo k škodlivému automatizovanému rozhodovaniu.

- **Podpora inovácií a technologického rozvoja** – nariadenie tiež deklaruje snahu Únie zaujať vedúcu pozíciu vo vývoji umelej inteligencie s dôrazom na etický a zodpovedný prístup. Z recitálu č. 143 možno odvodiť snahu Únie o podporu malých a stredných podnikov vrátane startupov. Akt o umelej inteligencii zavádza regulačné sandboxy na testovanie modelov umelej inteligencie v bezpečnom prostredí, čím vytvára podmienky pre testovanie bezpečnosti modelov pred ich uvedením do prevádzky.

- **Kategorizácia rizík** – nariadenie zavádza štyri stupne rizika.

  1. **Neprijateľné riziko = úplný zákaz**: Nariadenie zakazuje systémy, ktoré využívajú manipulatívne techniky alebo zneužívajú zraniteľnosť ľudí, systémy pre social scoring, biometrickú kategorizáciu citlivých znakov (napr. rasa či sexuálna orientácia) alebo systém hodnotenia rizika spáchania trestného činu len na základe profilu osoby. Zakázaná je aj nekontrolovaná hromadná extrakcia tvárových fotografií z internetu a niektoré formy vzdialenej biometrickej identifikácie, s výnimkou jej použitia pri pátraní po nezvestných osobách, prevencii terorizmu či pri vyšetrovaní závažných trestných činov.

  2. **Vysoké riziko (High-risk AI)**: Platí pre systémy, ktoré sú súčasťou bezpečnostných komponentov produktov podliehajúcich harmonizovanej legislatíve EÚ (napr. lekárske prístroje, vozidlá) alebo sú uvedené v prílohe č. III, napríklad:
     - systémy AI, ktoré sa majú používať na monitorovanie a zisťovanie zakázaného správania študentov počas skúšok v kontexte alebo v rámci inštitúcií vzdelávania a odbornej prípravy na všetkých úrovniach,
     - systémy AI, ktoré sa majú používať na nábor alebo výber fyzických osôb, najmä na umiestňovanie cielených inzerátov na pracovné miesta, na analýzu a filtrovanie žiadostí o zamestnanie a na hodnotenie uchádzačov,
     - systémy AI určené na rozpoznávanie emócií.

  3. **Obmedzené riziko (Limited risk)**: Ide najmä o systémy, ktoré interagujú priamo s ľuďmi (chatboty), generujú syntetický obsah (deepfake) alebo vykonávajú rozpoznávanie emócií či biometrickú kategorizáciu. Pre ne sú stanovené konkrétne transparenčné povinnosti (informovať používateľov, že komunikujú s AI, označiť syntetické výstupy, informovať osoby o použití biometrických a emocionálnych systémov a pod.).

  4. **Minimálne riziko (Minimal risk)**: Na systémy ako spamové filtre, prekladače alebo AI v počítačových hrách sa nariadenie nevzťahuje – majú len bežné povinnosti vyplývajúce z iných právnych predpisov.

- **Presadzovanie pravidiel a dohľad na ich dodržiavaním** – AI Act zriaďuje nový európsky orgán, ktorý bude dohliadať na dodržiavanie pravidiel a presadzovanie stanovených cieľov. Členské štáty sú tiež povinné zriadiť vnútroštátne dozorné orgány,

ktoré budú vybavovať sťažnosti a monitorovať dodržiavanie nariadenia povinnými subjektmi. Porušenie stanovených pravidiel podlieha sankciám.

2.1.3 Štruktúra AI Act

Nariadenie sa člení na 13 kapitol, ktoré spolu obsahujú 113 článkov. Každá kapitola reguluje iných okruh právnych vzťahov, od základných definícií až po dohľad a sankcie.

Prvá kapitola vymedzuje predmet a rozsah pôsobnosti nariadenia a jeho základné definície. Nariadenie sa vzťahuje na všetky modely umelej inteligencie uvedené na trh alebo uvedené do prevádzky v Európskej únii, bez ohľadu na pôvod modelu alebo jeho poskytovateľa. Široký rozsah pôsobnosti vymedzený článkom 2 má zabrániť obchádzaniu povinností podľa nariadenia.

Druhá kapitola sa týka zakázaných praktík využívajúcich AI. Táto kapitola obsahuje jediný článok, konkrétne článok 5, ktorý vymedzuje praktiky, ktoré sú v Európskej únii zakázané, pretože predstavujú neprijateľné riziko pre základné ľudské práva a hodnoty, na ktorých je Únia postavená. Zákaz týchto systémov vychádza z predpokladu, že predstavujú vysoké riziko zneužitia, napr. na automatizované hodnotenie, diskrimináciu alebo sledovanie jednotlivcov. Osobitnú skupinu tvoria systémy biometrickej identifikácie v reálnom čase na verejne prístupných miestach, ktoré je povolené len za účelom (i) cieleného pátrania po konkrétnych obetiach únosov, či nezvestných osobách, (ii) predchádzania konkrétnemu, závažnému a bezprostrednému ohrozeniu života alebo bezpečnosti fyzických osôb alebo skutočnej a existujúcej alebo skutočnej a predvídateľnej hrozbe teroristického útoku a (iii) lokalizácie alebo identifikácia osoby podozrivej zo spáchania trestného činu.

Tretia kapitola upravuje vysokorizikové systémy AI. Bol zavedený systém klasifikácie systémov umelej inteligencie podľa ich úrovne rizika, na základe ktorého je možné určiť primeranú úroveň regulácie podľa nariadenia. Systémy s vysokým rizikom podliehajú požiadavke systému riadenia rizík, bližšie upravenom v článku 9 (vzťahuje sa na ne povinné testovanie, osobitné podmienky pre správu údajov, vedenie záznamov a vypracovanie technickej dokumentácie). Tieto systémy musia byť zároveň dizajnované a vyvinuté tak, aby nad nimi počas obdobia ich používania mohli fyzické osoby vykonávať účinný dohľad, a to aj pomocou vhodných nástrojov rozhrania človek – stroj (čl. 14).

Aj **kapitolu IV** tvorí len jeden článok, konkrétne článok č. 50. Ten stanovuje povinnosti transparentnosti pre určité systémy umelej inteligencie, ktoré nepatria medzi vysoko rizikové. Hlavným cieľom týchto modelov je zabezpečiť informovanosť osôb o interakcii s umelou inteligenciou, čo v praxi znamená, že obsah vygenerovaný umelou inteligenciu by mal byť jasne označený (napr. deepfake a generatívne modely).

Piata kapitola reguluje modely AI pre všeobecné účely. Tieto modely nie sú špecializované na konkrétne účely, sú skôr širokospektrálne zamerané (napr. ChatGPT, DeepSeek či Copilot). Poskytovatelia podliehajú povinnostiam vrátane transparentnosti, bezpečnosti a zodpovednosti za dopady. Majú tiež povinnosť spracovávať riziká a monitorovať zneužitie.

Šiestu kapitolu tvoria opatrenia na podporu inovácií. Nariadenia zavádza povinnosť členských štátov zriadiť aspoň jedno regulačné experimentálne prostredie

pre AI na vnútroštátnej úrovni, ktoré bude uvedené do prevádzky do 2. augusta 2026 (tzv. regulačné sandboxy). Zmyslom sandboxov je overiť bezpečnosť a spoľahlivosť systémov pred ich uvedením na trh.

Siedma kapitola má názov Správa a riadenie. Zriaďuje sa Európska rada pre umelú inteligenciu, v ktorej má každý členský štát Únie jedného zástupcu. Rada pre AI poskytuje poradenstvo a pomoc Komisii a členským štátom s cieľom uľahčiť konzistentné a účinné uplatňovanie tohto nariadenia. Ďalej sa zriaďuje Poradné fórum, ktoré poskytuje technické odborné znalostí a poradenstvo rade pre AI a Komisii. Členovia poradného fóra predstavujú vyvážený výber zainteresovaných strán vrátane predstaviteľov priemyslu, **startupov, MSP**, občianskej spoločnosti a akademickej obce. Zloženie členov poradného fóra musí byť vyvážené, pokiaľ ide o komerčné a nekomerčné záujmy, a v rámci kategórie komerčných záujmov, pokiaľ ide o MSP a iné podniky s cieľom prispievať k plneniu ich úloh podľa nariadenia AI Act.

Ďalším orgánom je Vedecký panel nezávislých expertov, ktorý pozostáva z expertov vybraných Komisiou na základe aktuálnych vedeckých alebo technických odborných znalostí v oblasti AI. Členské štáty sú tiež povinné určiť aspoň jeden notifikujúci orgán a aspoň jeden orgán dohľadu nad trhom.

Kapitola VIII stanovuje, že vysokorizikové systémy podliehajúce povinnej registrácii, budú uložené v databáze Únie pre vysokorizikové systémy AI. Databáza bude verejne prístupná a poskytovatelia alebo oprávnení zástupcovia do nej budú vkladať údaje o svojich systémoch umelej inteligencie. Účelom databázy je zvýšiť úroveň transparentnosti a zabezpečiť účinný dohľad nad rizikovými systémami AI.

Kapitola IX sa zaoberá monitorovaním po uvedení na trh, vrátane povinností poskytovateľov a regulačných orgánov. Zber údajov o systéme v reálnom čase preventívne minimalizuje možnosť výskytu incidentov. Ďalšia časť tejto kapitoly sa zaoberá výmenou informácií medzi členskými štátmi a regulačnými orgánmi. Táto požiadavka pomáha zabezpečiť konzistentnosť regulácie v celej Európskej únii. Dozor nad trhom je poslednou časťou, v ktorej nariadenie posilňuje právomoci regulačných orgánov možnosťou ukladať sankcie za porušenie pravidiel.

Kódexy správania a usmernenia sú uvedené v **kapitole X**. Ide o spôsob regulácie systémov, ktoré nepatria do skupiny s vysokým rizikom, podobným spôsobom ako systémy, ktoré do tejto skupiny patria, avšak v zásade na báze dobrovoľnosti. Kódexy umožňujú zavedenie postupov na zabezpečenie dobrovoľného, etického a bezpečného používania umelej inteligencie. Nariadenie povzbudzuje jednotlivé regulačné orgány, aby podporovali kódexy správania. Takéto kódexy by mali obsahovať kľúčové zásady, ako sú dôveryhodnosť, transparentnosť, zodpovednosť a prevencia diskriminácie.

Usmernenia Komisie, ktoré tvoria druhú časť tejto kapitoly, slúžia na praktické vykonávanie tohto nariadenia **so zvláštnym zreteľom na malé a stredné podniky**. Úrad pre AI a členské štáty pri podpore a uľahčovaní vypracúvania kódexov správania **zohľadňujú osobitné záujmy a potreby MSP** vrátane startupov.

Rovnako tak Komisia pri vydávaní usmernení **venuje osobitnú pozornosť potrebám MSP** vrátane startupov.

Kapitola XI sa zaoberá pravidlami delegovania právomocí na Európsku komisiu a postupom výboru. Komisia je oprávnená prijímať delegované akty, najmä za účelom aktualizovania technologických príloh. Táto právomoc je obmedzená od 01.08.2024 na obdobie piatich rokov s možnosťou automatického predĺženia. Diskusie vo výboroch umožňujú transparentné a centralizované rozhodovanie s cieľom zohľadniť názory členských štátov.

Predposledná **kapitola s číslom XII** upravuje sankcie iné donucovacie opatrenia. Sankcie môžu zahŕňať rôzne opatrenia presadzovania, napríklad varovania či nepeňažné opatrenia. Nariadenia však umožňuje regulátorovi uložiť pokutu až do výšky 7 % celosvetového ročného obratu.

Kapitolu XIII tvoria záverečné ustanovenia.

2.1.4 Definície a kategorizácia AI systémov

Nariadenie o umelej inteligencii stanovuje právne záväznú definíciu systému umelej inteligencie, ktorá je kľúčová pre určenie rozsahu povinností jednotlivých subjektov. Podľa článku 3 ods. 1 nariadenia sa systém umelej inteligencie definuje ako *„strojový systém, ktorý je dizajnovaný na prevádzku s rôznymi úrovňami autonómnosti, ktorý môže po nasadení prejavovať adaptabilitu a ktorý pre explicitné alebo implicitné ciele odvodzuje zo vstupov, ktoré dostáva, spôsob generovania výstupov, ako sú predpovede, obsah, odporúčania alebo rozhodnutia, ktoré môžu ovplyvniť fyzické alebo virtuálne prostredie“.*

Táto definícia odráža dynamiku vývoja technológie umelej inteligencie a odlišuje umelú inteligenciu od bežných softvérových aplikácií tým, že zdôrazňuje jej schopnosť generovať výstupy na základe spracovania vstupov.

Definícia v tomto nariadení bola vytvorená s cieľom harmonizácie s medzinárodnými normami, najmä s normami prijatými Organizáciou pre hospodársku spoluprácu a rozvoj a Európskou komisiou na základe skorších stratégií v oblasti umelej inteligencie. Kľúčovým aspektom tejto definície je odlíšenie od jednoduchých automatizovaných systémov, ktoré fungujú na základe vopred definovaných pravidiel a nemajú schopnosť prispôsobovať sa.

Toto nariadenie zavádza prístup, ktorý je založený na posúdení miery rizika. Prísnejšie pravidlá sa uplatňujú predovšetkým na najrizikovejšie technológie. Jednotlivé typy systémov sa potom analyzujú podľa ich rizikovosti.

2.1.5 Zakázané systémy

Tieto systémy podliehajú najvyššej regulácii, pretože predstavujú najvyššie riziko pre základné práva a hodnoty Európskej únie. Nariadenie tieto systémy definuje v článku 5, pričom ich explicitne zakazuje. Tento zákaz zároveň znamená zákaz vývoja takéhoto systému a jeho uvádzania na trh v rámci EÚ. Medzi zakázané systémy patria systémy, ktoré používajú manipulatívne techniky na ovplyvňovanie správania jednotlivcov prostredníctvom podprahových signálov alebo iných prostriedkov takým spôsobom, ktorý oslabuje ich schopnosť prijímať nezávislé rozhodnutia. Zakázané sú aj systémy, ktoré podporujú hodnotenie „sociálneho skóre“, t. j. automatizované hodnotenie jednotlivcov podľa rôznych kritérií, najmä osobnostných charakteristík či spoločenského správania.

Cieľom tohto obmedzenia je zabezpečiť ochranu základných ľudských práv, najmä ochranu súkromia a zákaz diskriminácie, ale tiež zabezpečiť ochranu pred zneužívaním týchto technológií na štátnu represiu či hromadné sledovanie.

2.1.6 Vysokorizikové systémy

Vysokorizikové systémy sa vyznačujú vysokou mierou potenciálneho negatívneho dopadu na práva osôb, preto ich možno používať, vyvíjať či uvádzať na trh len po splnení pomerne prísnych legislatívnych podmienok.

Zmyslom osobitných pravidiel pre vysokorizikové systémy je zabezpečiť, aby AI v citlivých oblastiach nevytvárala neprimerané riziká pre verejné záujmy chránené právom EÚ, najmä tam, kde sa môže dotýkať základných práv garantovaných Chartou základných práv EÚ (napr. ľudská dôstojnosť, súkromie a rodinný život, ochrana osobných údajov, prístup k informáciám, právo na vzdelanie či ochrana spotrebiteľa).

AI Act rozlišuje dve skupiny vysokorizikových AI systémov**. Nariadenie rozlišuje, či rizikovosť vychádza** z **povahy produktu**, do ktorého je AI integrovaná, alebo zo **spoločensky citlivého použitia** AI v určitých oblastiach a konkrétnych situáciách. Tomu zodpovedajú dve základné kategórie.

Vysokorizikové systémy podľa článku 6 ods. 1 (AI ako bezpečnostný komponent produktu alebo produkt samotný)
Za vysokorizikový sa považuje AI systém vtedy, ak je určený na použitie ako bezpečnostná súčasť produktu (alebo je sám takýmto produktom) spadajúceho pod harmonizačné právne predpisy EÚ uvedené v prílohe I, a zároveň sa dotknutý produkt (resp. samotný AI systém ako produkt) musí pred uvedením na trh alebo do prevádzky podrobiť **posúdeniu zhody treťou stranou** podľa príslušných harmonizačných predpisov.

Vysokorizikové systémy podľa článku 6 ods. 2 (systémy uvedené v prílohe III)
Podľa článku 6 ods. 2 AI Act sa režim vysokorizikových systémov nevzťahuje iba na AI, ktorá tvorí bezpečnostnú súčasť regulovaných výrobkov alebo je sama takýmto výrobkom. Za vysokorizikové môžu byť označené aj ďalšie AI systémy, pokiaľ sú zaradené do zoznamu v prílohe III AI Act.

Typicky ide o samostatné AI systémy, pri ktorých použitie v určitej oblasti môže mať významný dopad na zdravie, bezpečnosť alebo základné práva dotknutých osôb. Pri hodnotení rizikovosti sa berie do úvahy najmä intenzita možnej ujmy, pravdepodobnosť jej vzniku a tiež to, či sa systém nasadzuje v jednej alebo viacerých konkrétne vymedzených oblastiach, ktoré nariadenie detailne opisuje.

Zaradenie systému do kategórie vysokorizikových vychádza z metodiky a hodnotiacich kritérií, ktoré má Európska komisia uplatňovať aj pri **budúcich aktualizáciách** zoznamu.

Súčasne však AI Act stanovuje, že ani samotné uvedenie AI systému v prílohe III ešte automaticky neznamená, že v každom prípade pôjde o vysokorizikový systém. Ak konkrétny systém **nepredstavuje významné riziko** ujmy na zdraví, bezpečnosti alebo základných

právach fyzických osôb, za vysokorizikový sa nepovažuje. Táto možnosť vylúčenia sa však neuplatní, pokiaľ systém **vykonáva profilovanie** fyzických osôb.[4]

Za vysokorizikové systémy sa tak považujú systémy AI v oblastiach ako biometria (diaľková identifikácia osôb a rozpoznávanie emócií), kritická infraštruktúra (systémy riadiace dopravu, zásobovanie energiami), ľudské zdroje (najmä nábor nových zamestnancov), migrácia (posudzovanie žiadostí o azyl) a pod.

2.1.7 Systémy s obmedzenými regulačnými požiadavkami

Do tejto kategórie patria AI systémy, ktoré nie sú priamou hrozbou pre používateľa, avšak existuje tu určité riziko zavádzania alebo zneužitia. Preto sa na ne typicky uplatňuje najmä požiadavka transparentnosti. Ide najmä chatboty, pri ktorých má poskytovateľ povinnosť používateľa zrozumiteľne informovať, že komunikuje s umelou inteligenciou. Podobne pri generovanom obsahu, vrátane „deepfake“ technológií, musí byť obsah označený ako vytvorený umelou inteligenciou.

Zmyslom je umožniť používateľovi správne posúdiť dôveryhodnosť a povahu výstupu a zabrániť skrytému alebo klamlivému použitiu AI.

Hoci ide o „najľahší“ regulačný režim, aj tu môže nedodržanie transparentnosti viesť k sankciám.

2.1.8 Systémy s minimálnym rizikom

Tieto systémy môžu byť vyvíjané a používané prakticky bez obmedzení, pretože nepredstavujú riziko zásahu do základných práv užívateľov. Do tejto kategórie spadajú napríklad systémy na personalizáciu reklamy, inteligentní asistenti či rôzne analytické nástroje.

2.2 Nariadenie (EÚ) 2024/2847 – Cyber Resilience Act (CRA)

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti) (Text s významom pre EHP) (ďalej aj ako „CRA“) je právnou normou, ktorej cieľom je posilniť kybernetickú bezpečnosť produktov s digitálnymi prvkami, ktoré sú uvádzané na trh v rámci EÚ.

Toto nariadenie sa zameriava na zabezpečenie jednotného prístupu k bezpečnosti naprieč celým jednotným trhom a prináša záväzné požiadavky na výrobcov, distribútorov a ďalšie hospodárske subjekty. CRA je reakciou na rastúci počet kybernetických útokov a zraniteľností, ktoré ovplyvňujú fyzické aj právnické osoby naprieč EÚ.

[4] https://www.epravo.sk/top/clanky/co-su-vysokorizikove-ai-systemy-podla-ai-act-a-ake-povinnosti-z-nich-vyplyvaju-6454.html

Cieľom tohto nariadenia je nastaviť jednotný rámec regulujúci vývoj bezpečných produktov s digitálnymi prvkami a ich uvádzanie na trh tak, aby sa do obehu dostávali hardvérové a softvérové riešenia s čo najnižším počtom zraniteľností a aby výrobcovia pristupovali ku kybernetickej bezpečnosti zodpovedne **počas celého životného cyklu produktu**. Zároveň má nariadenie vytvoriť predpoklady, aby používatelia vedeli pri výbere a používaní takýchto produktov reálne zohľadniť aj ich kybernetickú bezpečnosť – napríklad tým, že sa zvýši transparentnosť informácií o tom, ako dlho bude produkt na trhu podporovaný, vrátane bezpečnostných aktualizácií.

Aj toto nariadenie v jednom zo svojich úvodných recitálov deklaruje **zámer pomôcť malým a stredným podnikom.** Podľa recitálu 6 *„Komisia by pri uplatňovaní tohto nariadenia mala poskytnúť usmernenia na pomoc hospodárskym subjektom, najmä mikropodnikom a malým a stredným podnikom. Takéto usmernenia by sa mali okrem iného týkať rozsahu pôsobnosti tohto nariadenia, najmä spracúvania údajov na diaľku a jeho dôsledkov pre vývojárov slobodného softvéru a softvéru s otvoreným zdrojovým kódom, uplatňovania kritérií používaných na určenie období podpory pre produkty s digitálnymi prvkami, vzájomného pôsobenia medzi týmto nariadením a inými právnymi predpismi Únie a koncepcie podstatnej úpravy.“*

Cieľom tohto nariadenia je tiež dosiahnuť vysokú úroveň kybernetickej bezpečnosti produktov s digitálnymi prvkami, ako aj ich integrovaných riešení spracúvania údajov na diaľku. Za takéto „spracúvanie údajov na diaľku“ sa má považovať len spracovanie, ktoré je určené a vyvinuté výrobcom (alebo v jeho mene) pre konkrétny produkt, pričom bez tejto vzdialenej funkcionality by produkt nevedel vykonávať aspoň jednu zo svojich funkcií.

Takto nastavené vymedzenie má zabezpečiť, aby výrobca primerane a komplexne zabezpečil produkt bez ohľadu na to, či sa údaje spracúvajú alebo ukladajú priamo v zariadení používateľa alebo na diaľku u výrobcu. Zároveň platí, že vzdialené spracúvanie alebo uchovávanie údajov spadá do pôsobnosti nariadenia iba vtedy, ak je nevyhnutné na to, aby produkt plnil svoje funkcie.

Typickým príkladom je situácia, keď mobilná aplikácia potrebuje prístup k aplikačnému rozhraniu (API) alebo databáze poskytovanej ako služba, ktorú vyvinul výrobca – vtedy sa aj táto služba považuje za riešenie spracúvania údajov na diaľku v zmysle nariadenia. Z toho zároveň vyplýva, že požiadavky kladené na takéto riešenia sa nevzťahujú na všeobecné technické, prevádzkové či organizačné opatrenia, ktorými výrobca riadi riziká bezpečnosti svojich sietí a informačných systémov ako celku.

Možno súhrnne konštatovať, že CRA sa vzťahuje na produkty s digitálnymi prvkami, ktoré sú pripojené k internetu alebo iným zariadeniam, a zahŕňa široké spektrum technológií vrátane:

- IoT (Internet of Things) zariadení, ako sú inteligentné hodinky, fitness náramky, chladničky, TV a kamery,
- softvérových aplikácií vrátane bezpečnostných nástrojov ako antivírusové programy a VPN,
- hardware komponentov, ako sú mikroprocesory, sieťové smerovače, základné dosky, modemy.

Obdobie podpory, počas ktorého je výrobca povinný zabezpečiť účinné riešenie zraniteľností, by nemalo byť kratšie ako päť rokov, pokiaľ životnosť produktu s digitálnymi prvkami nie je kratšia ako päť rokov, pričom v takom prípade by mal výrobca zabezpečiť riešenie zraniteľností počas tejto životnosti.

Ak sa dôvodne očakáva, že produkt s digitálnymi prvkami sa bude používať dlhšie ako päť rokov, a to nielen v prípade hardvérových komponentov, ale aj v prípade softvéru (operačné systémy alebo nástroje na editovanie videí), výrobcovia by mali zabezpečiť dlhšie obdobia podpory.

Na tomto mieste je ešte potrebné zdôrazniť, že nariadenia CRA a AI Act sú vzájomne prepojené a dopĺňajú sa, pričom sa výslovne odvolávajú jedno na druhé. Spoločným účelom obidvoch nariadení je zabezpečiť kybernetickú bezpečnosti (nielen) vysokorizikových systémov AI.

AI Act kladie na vysokorizikové systémy umelej inteligencie prísne požiadavky vrátane technickej a organizačnej bezpečnosti. Podľa článku 15 AI Act musia byť tieto systémy „dizajnované a vyvinuté tak, aby dosahovali primeranú úroveň presnosti, spoľahlivosti a kybernetickej bezpečnosti a aby v týchto ohľadoch fungovali konzistentne počas celého svojho životného cyklu.“ AI Act tak v zásade **vyžaduje, aby tieto vysokorizikové systémy odolali** neoprávneným zásahom tretích strán.

Vzťah medzi CRA a AI Act pritom možno najlepšie vysvetliť s poukazom na článok **12 CRA**, v zmysle ktorého dotknutý vysokorizikový AI systém spĺňa požiadavky kybernetickej bezpečnosti, ak:

- spĺňa základné požiadavky kybernetickej bezpečnosti stanovené v časti I prílohy I CRA;
- procesy zavedené výrobcom/poskytovateľom sú v súlade so základnými požiadavkami kybernetickej bezpečnosti stanovenými v časti II prílohy I CRA, a súčsne
- dosiahnutie úrovne ochrany kybernetickej bezpečnosti požadovanej podľa článku 15 AI Act musí byť preukázané v EÚ vyhlásení o zhode vydanom podľa CRA.

Uvedené prepojenie obidvoch nariadené EÚ má svoje opodstatnenie. Zabezpečí sa tým, že systémy AI budú podliehať ucelenému a jednotnému režimu kybernetickej bezpečnosti.

Medzi kľúčové povinnosti jednotlivých hospodárskych subjektov patrí:

- **Výrobcovia (čl. 13):**
  a) musia navrhnúť a vyrábať produkty s dôrazom na bezpečnosť, pred uvedením na trh vykonať posúdenie kybernetických rizík a zabezpečiť pravidelné aktualizácie,
  b) sú povinní monitorovať zraniteľnosti produktov a v prípade zistenia nedostatkov okamžite informovať regulačné orgány a používateľov,
  c) sú povinní pri integrácii komponentov získaných od tretích strán uplatňovať náležitú starostlivosť,

d) ohlasovacie povinnosti pri zneužití zraniteľnosti produktu či závažnom incidente podľa čl. 14.

- **Dovozcovia a distribútori (čl. 19 a 20):**
  a) musia overiť, že produkty, ktoré uvádzajú na trh, spĺňajú požiadavky CRA, pričom uvedené zahŕňa zabezpečenie súladu s bezpečnostnými normami a príslušnými certifikátmi,
  b) musia aktívne sledovať oznámenia od výrobcov a zabezpečiť, aby boli všetky bezpečnostné aktualizácie a opatrenia komunikované zákazníkom.

- **Notifikované osoby a certifikačné orgány (čl. 47):**
  CRA vyžaduje, aby určité produkty podliehali posúdeniu zhody treťou stranou. Certifikačné orgány zohrávajú kľúčovú úlohu v posudzovaniu zhody so základnými požiadavkami na kybernetickú bezpečnosť.

2.3 Smernica (EÚ) 2022/2555 – NIS2

Smernica NIS2 nadväzuje na prvú „NIS smernicu“ (smernica (EÚ) 2016/1148) pričom vychádza z predpokladu, že model regulácie nastavený prvou smernicou už nie je dostatočný na dosiahnutie požadovanej úrovne kybernetickej bezpečnosti v EÚ. Neaktuálnym sa stalo najmä členenie regulovaných subjektov a nejednotnosť regulácie naprieč členskými štátmi EÚ.

Pôvodné rozlišovanie medzi „prevádzkovateľmi základných služieb“ a „poskytovateľmi digitálnych služieb“ sa postupne stalo neaktuálnym, pretože už nezodpovedalo reálnemu významu sektorov a služieb pre fungovanie spoločnosti a hospodárstva vnútorného trhu. NIS2 preto výslovne smeruje k odstráneniu nedostatkov tohto rozlišovania a k modernejšiemu konceptu regulovaných kategórií subjektov.

Pôvodná smernica NIS1 tiež ponechávala členským štátom široký priestor pri identifikácii subjektov, ktoré budú regulované (najmä pri „prevádzkovateľoch základných služieb“). To viedlo k veľkým rozdielom medzi členskými štátmi a k právnej neistote.

Cieľom bolo, aby sa rozsah uplatňovania podľa odvetví rozšíril na väčšiu časť hospodárstva, aby boli komplexne pokryté odvetvia a služby, ktoré majú zásadný význam pre kľúčové spoločenské a hospodárske činnosti v rámci vnútorného trhu. Smernica NIS2 si tak kladie za cieľ odstrániť nedostatky v rozlišovaní medzi prevádzkovateľmi základných služieb a poskytovateľmi digitálnych služieb, ktoré, ako sme už uviedli vyššie, sa ukázalo ako zastarané, pretože neodráža význam odvetví alebo služieb pre spoločenské a hospodárske činnosti na vnútornom trhu.

2.3.1 Novela zákona o kybernetickej bezpečnosti

Dňa 1. januára 2025 nadobudla účinnosť novela zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, ktorá do právneho poriadku Slovenskej republiky transponuje smernicu NIS2. Novela zákona o kybernetickej bezpečnosti prináša rozšírenie počtu subjektov, na ktoré sa zákon vzťahuje. Ide o spoločnosti (organizácie), ktorých predmet činnosti spadá pod novo regulované oblasti, ako je odpadové hospodárstvo, potravinárstvo či výroba.

Národný bezpečnostný úrad Slovenskej republiky odhaduje, že počet týchto subjektov presahuje 6.000.

Aby spoločnosť (organizácia) zistila, či spadá pod nové pravidlá na zvýšenie úrovne kybernetickej bezpečnosti, musí si v prvom rade zodpovedať otázku, či je prevádzkovateľom tzv. základnej služby.

Novela explicitne určuje, kto sa **do registra prevádzkovateľov základných služieb (PZS) zapisuje.**

Za prevádzkovateľa základnej služby sa po novom považujú organizácie, ktoré sú aspoň stredným podnikom a súčasne ktoré vykonávajú činnosti v sektoroch uvedených v Prílohe č. 1 a č. 2 zákona.

Ide o vysoko kritické sektory ako energetika, doprava, financie, zdravotníctvo, voda, digitálna infraštruktúra, verejná správa a vesmír, ale aj iné kritické novo regulované sektory, ako poštové služby, odpadové hospodárstvo, kuriérske služby, výroba a distribúcia chemických látok, potravinárstvo a výroba a výskum.

Do registra sa zapisujú aj ústredné orgány štátnej správy, kritické subjekty a ďalšie subjekty, ktoré vykonávajú činnosti v kľúčových oblastiach ako verejná elektronická komunikácia, správa doménových názvov alebo poskytovanie kritických služieb s vplyvom na verejný poriadok alebo bezpečnosť.

Subjekty ako

- ústredné orgány štátnej správy a iné štátny orgán s celoštátnou pôsobnosťou,
- kritické subjekty,
- štátne orgány vykonávajúce pôsobnosť v najmenej dvoch okresoch a vyšší územný celok, ak by narušenie ich činnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- mestá, ak by narušenie výkonu jeho pôsobnosti mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie,
- správca ITVS po predchádzajúcej konzultácii s príslušným ústredným orgánom
- osoby, ktoré poskytujú služby registrácie názvu domény bez ohľadu na splnenie podmienok veľkosti pre stredný podnik,

sa do registra PZS zapisujú bez ohľadu na sektor, v ktorom pôsobia.

Je podstatné, aby dotknuté subjekty túto právnu reguláciu dobre poznali, pretože každá organizácia musí sama zhodnotiť, či spĺňa vyššie uvedené kritéria a vykonáva dané činnosti. V rozhodovaní subjektom pomôže indikatívna pomôcka NBÚ, dostupná na: https://nis2.nbu.gov.sk/indikativna-pomocka-na-urcenie-subjektu-ako-poskytovatela-zakladnej-sluzby/.

Povinnosti prevádzkovateľov základných služieb

- **Oznámenie na NBÚ a zápis do registra PZS**

Každý subjekt, ktorý sa identifikuje ako prevádzkovateľ základnej služby, musel na NBÚ podať oznámenie o vykonávaní činnosti podľa zákona o kybernetickej bezpečnosti do 03.03.2025. Ak sú splnené zákonné podmienky pre zápis do registra, NBÚ doň subjekt zapíše. Od momentu zápisu vznikajú organizácii nové povinnosti ako prevádzkovateľovi základnej služby.

- **Bezpečnostné opatrenia**

Každý subjekt je povinný do 12 mesiacov od zápisu do registra prevádzkovateľom základnej služby prijať všeobecné bezpečnostné opatrenia podľa § 20 zákona.

Povinnosťou prevádzkovateľa základnej služby pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, je uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa zákona a tretia strana je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia v súlade s touto zmluvou.

Vzor zmluvy pripravil Národný bezpečnostný úrad SR na svojom webovom sídle a je dostupný na https://www.nbu.gov.sk/bezpecnostne-opatrenia/.

- **Audit kybernetickej bezpečnosti**

Do 24 mesiacov odo dňa zápisu do registra PZS (a následne v periodicite podľa vyhlášky) je každý subjekt povinný vykonať audit kybernetickej bezpečnosti alebo tzv. samohodnotenie. Audit kybernetickej bezpečnosti môže vykonať len certifikovaný audítor kybernetickej bezpečnosti. Samohodnotenie namiesto auditu môžu vykonať tie subjekty, ktoré nie sú prevádzkovateľom kritickej základnej služby. Avšak aj v prípade samohodnotenia bude musieť takýto subjekt vykonať prvý audit prostredníctvom certifikovaného audítora do 5 rokov a potom v periodicite podľa vyhlášky.

- Ďalšie povinnosti PZS sú nasledovné:
  - Určiť manažéra kybernetickej bezpečnosti,
  - Implementovať procesy pre informovanie štatutárneho orgánu o otázkach kybernetickej bezpečnosti,
  - Realizovať hlásenia závažných kybernetických bezpečnostných incidentov a to prostredníctvom jednotného informačného systému kybernetickej bezpečnosti,
  - Dbať o bezpečnosť dodávateľského reťazca a pre tento účel uzatvoriť zmluvu s tretími stranami, ktoré zabezpečujú služby súvisiace s kybernetickou bezpečnosťou.

3 PRIAME DOPADY REGULÁCIÍ NA MSP

Nové technologické regulácie Európskej únie predstavujú pre MSP významnú zmenu podnikateľského prostredia. Táto kapitola analyzuje priame dopady AI Act, Cyber Resilience Act a NIS2 na MSP z hľadiska nákladov na súlad, administratívnej záťaže, personálnych a technologických požiadaviek a hodnotí pomer a súlad nákladov a prínosov.

3.1 Náklady na súlad (compliance)

Náklady na dosiahnutie súladu s novými reguláciami predstavujú pre MSP jeden z najvýznamnejších priamych dopadov. Tieto náklady zahŕňajú investície do systémov, procesov, dokumentácie, certifikácie a priebežnej údržby compliance programov. Výška nákladov sa výrazne líši v závislosti od typu regulácie, veľkosti podniku, odvetvia a aktuálnej úrovne pripravenosti na nové požiadavky.

3.1.1 Náklady na súlad s AI Act

AI Act sa vzťahuje na MSP v rôznych rolách v závislosti od spôsobu využívania umelej inteligencie. Regulácia rozlišuje medzi poskytovateľmi (providers), ktorí vyvíjajú alebo uvádzajú AI systémy na trh, a nasadzovateľmi (deployers), ktorí AI systémy používajú v rámci svojej podnikateľskej činnosti. Medzi typické prípady MSP dotknutých AI Act patria:

- Podniky využívajúce AI na komunikáciu so zákazníkmi (chatboty, virtuálni asistenti, automatizované zákaznícke linky)
- Spoločnosti prijímajúce automatizované rozhodnutia pomocou AI (napr. vyhodnocovanie životopisov a výber kandidátov v HR procesoch)
- Subjekty generujúce obsah pomocou AI (texty, obrázky, video, marketingové materiály)
- Vývojári AI systémov pre špecifické vertikálne riešenia (zdravotníctvo, finančné služby, vzdelávanie)
- Priemyselné podniky využívajúce AI na prediktívnu údržbu, kontrolu kvality alebo optimalizáciu procesov.

Pre MSP, ktoré vyvíjajú alebo uvádzajú na trh vysokorizikové AI systémy, sú náklady na compliance najvyššie. Podľa štúdie CEPS (Centre for European Policy Studies) môžu náklady na zriadenie úplne nového systému riadenia kvality (Quality Management System - QMS) dosiahnuť 193 000 až 330 000 EUR, s dodatočnými ročnými nákladmi na údržbu približne 71 400 EUR. Tieto náklady sú relevantné najmä pre podniky, ktoré doposiaľ nemali zavedený žiadny formalizovaný QMS.[5]

Celkové náklady na compliance pre jeden vysokorizikový AI systém sa odhadujú na 9 500 až 14 500 EUR, pričom zahŕňajú náklady na posúdenie zhody (3 500 – 7 500 EUR) a splnenie technických požiadaviek (6 000 - 7 000 EUR). Podľa analýzy Intellera Consulting môžu celkové náklady na compliance pre komplexnejšie prípady dosiahnuť až 301 200 EUR,

[5] **Renda, Andrea; Schrefler, Lorna; Bontoux, Laurent et al.** *Study to Support an Impact Assessment of Regulatory Requirements for Artificial Intelligence in Europe.* Centre for European Policy Studies (CEPS), 2021

pričom využitie podporných služieb ako European Digital Innovation Hubs (EDIHs) alebo Testing and Experimentation Facilities (TEFs) môže tieto náklady znížiť na približne 229 444 EUR.[6]

MSP, ktoré AI systémy len využívajú (nasadzujú), ale nevyvíjajú, čelia nižším, avšak stále významným nákladom. Tieto zahŕňajú najmä zabezpečenie ľudského dohľadu nad vysokorizikovými AI systémami, školenia zamestnancov v oblasti AI gramotnosti (povinnosť účinná od februára 2025), monitorovanie výstupov AI systémov a uchovávanie logov. Pre transparentné AI systémy (chatboty, generátory obsahu) ide predovšetkým o náklady na implementáciu informačných povinností voči používateľom.

AI Act obsahuje osobitné ustanovenia na zníženie záťaže pre MSP. Európska komisia pripraví zjednodušené formuláre technickej dokumentácie pre malé podniky a mikropodniky. Poplatky za posúdenie zhody budú proporcionálne znížené v závislosti od veľkosti a trhového podielu podniku. MSP majú prioritný bezplatný prístup do regulačných sandboxov, ktoré umožňujú testovanie AI systémov v kontrolovanom prostredí pod dohľadom regulátora. Pri sankciách platí pre MSP princíp „nižšia z hodnôt“ namiesto „vyššia z hodnôt“, čo znižuje maximálne možné pokuty.

3.1.2 Náklady na súlad s Cyber Resilience Act

Cyber Resilience Act zavádza horizontálne požiadavky na kybernetickú bezpečnosť pre všetky produkty s digitálnymi prvkami uvádzané na trh EÚ. Pre MSP pôsobiace ako výrobcovia, dovozcovia alebo distribútori softvérových a hardvérových produktov to znamená potrebu zásadných investícií do bezpečnosti produktov počas celého ich životného cyklu.

Podľa odhadov Európskej komisie môžu celkové náklady na compliance pre výrobcov dosiahnuť až 29 miliárd EUR na úrovni EÚ. Pre jednotlivé MSP sa náklady líšia v závislosti od kategórie produktu. Odborníci odhadujú, že implementácia CRA požiadaviek môže zvýšiť náklady na vývoj softvéru približne o 15 %. Hlavné nákladové položky zahŕňajú:[7]

- **Security by design a security by default** - Náklady na integráciu bezpečnosti do návrhu produktov od počiatočných fáz vývoja, vrátane bezpečných predvolených nastavení a eliminácie slabých hesiel
- **Hodnotenie a riadenie rizík** - Implementácia procesov na identifikáciu a riadenie kybernetických rizík pred uvedením produktu na trh
- **Penetračné testovanie** - Pravidelné bezpečnostné testy produktov na identifikáciu zraniteľností (typicky 5 000 - 50 000 EUR za test v závislosti od komplexnosti)
- **Software Bill of Materials (SBOM)** - Vytvorenie a údržba detailného zoznamu všetkých komponentov produktu vrátane open-source závislostí
- **Bezpečnostné aktualizácie** - Zabezpečenie automatických bezpečnostných aktualizácií po dobu minimálne 5 rokov od uvedenia na trh

[6] **Intellera Consulting.** *The economic impact of the Artificial Intelligence Act on European SMEs.* Study for the European Commission, 2022.

[7] **European Commission.** *Impact Assessment Report accompanying the Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).* SWD(2022) **European Commission.** *Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)*

- **Správa zraniteľností** - Procesy na prijímanie hlásení o zraniteľnostiach, ich vyhodnocovanie a riešenie
- **Dokumentácia a uchovávanie záznamov** - Technická dokumentácia musí byť uchovávaná 10 rokov po uvedení produktu na trh alebo počas celej doby podpory.

Väčšina produktov (približne 90 %) bude spadať do kategórie 'default', kde postačuje sebahodnotenie výrobcom. Pre produkty kategórie 'Important' (Class I a II) a 'Critical' bude potrebné posúdenie treťou stranou (notifikovaným orgánom), čo zvyšuje náklady o ďalších 5 000 - 25 000 EUR v závislosti od komplexnosti produktu.[8]

Náklady na hlásenie incidentov: Od 11. septembra 2026 budú výrobcovia povinní hlásiť aktívne zneužívané zraniteľnosti a závažné bezpečnostné incidenty agentúre ENISA do 24 hodín. Toto si vyžaduje investície do monitorovacích systémov a procesov na detekciu a eskaláciu incidentov. Nesplnenie požiadaviek CRA môže viesť k pokutám až do výšky 15 miliónov EUR alebo 2,5 % celosvetového ročného obratu.

3.1.3 Náklady na súlad s NIS2

Smernica NIS2 sa primárne vzťahuje na stredné a veľké podniky v regulovaných sektoroch. Na Slovensku sa podľa dôvodovej správy k novele zákona o kybernetickej bezpečnosti dotýka minimálne 3 403 organizácií. Pre MSP sú relevantné najmä nepriame dopady cez dodávateľský reťazec, avšak stredné podniky (50-249 zamestnancov) v regulovaných sektoroch spadajú priamo pod NIS2.

Podľa štúdie Frontier Economics môže implementácia NIS2 zvýšiť vstupné náklady dotknutých sektorov celkovo o 23,4 miliardy EUR na úrovni EÚ. Pre individuálne stredné podniky sa odhady celkových nákladov na compliance pohybujú medzi 200 000 a 500 000 EUR. Podľa prieskumu ENISA z roku 2024 očakáva väčšina organizácií jednorazové alebo trvalé navýšenie rozpočtov na kybernetickú bezpečnosť v súvislosti s NIS2. Celkovo sa predpokladá nárast nákladov o 12 až 22 % v závislosti od toho, či podnik už spadal pod pôvodnú smernicu NIS.[9]

Prieskum ENISA tiež odhalil, že stredné podniky môžu potrebovať 1 250 až 2 500 hodín ročne na zabezpečenie súladu s NIS2, s odhadovanými ročnými nákladmi približne 30 000 EUR. Pre malé podniky sa odhady pohybujú na úrovni 300 až 800 hodín ročne s nákladmi 1 000 až 20 000 EUR. Je však potrebné poznamenať, že 34 % MSP podľa prieskumu ENISA nebude schopných získať potrebný rozpočet na implementáciu NIS2 požiadaviek.

Hlavné nákladové položky NIS2 compliance:

- **Bezpečnostné technológie -** Implementácia systémov na detekciu a prevenciu prienikov (IDS/IPS), SIEM riešení, šifrovania, zálohovacích a recovery systémov

[8] **European Commission.** *Impact Assessment Report accompanying the Proposal for a Regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).* SWD(2022)
[9] **Frontier Economics.** *The economic impact of the NIS2 Directive.* Study prepared for the European Commission, 2022

- **Riadenie rizík -** Analýza rizík, hodnotenie hrozieb, implementácia opatrení na ich mitigáciu
- **Incident response -** Vytvorenie procesov a systémov na detekciu, reakciu a hlásenie bezpečnostných incidentov
- **Kontinuita podnikania -** Plánovanie krízového riadenia a zabezpečenie kontinuity prevádzky
- **Bezpečnosť dodávateľského reťazca -** Audit a riadenie bezpečnosti dodávateľov a partnerov
- **Školenia zamestnancov -** Pravidelné vzdelávanie v oblasti kybernetickej bezpečnosti pre všetkých zamestnancov vrátane vrcholového manažmentu
- **Poistenie kybernetických rizík -** Podľa ENISA má v súčasnosti kybernetické poistenie len 13 % MSP, pričom náklady na poistné sa pohybujú od niekoľkých tisíc do desiatok tisíc EUR ročne v závislosti od pokrytia

3.2 Administratívna a byrokratická záťaž

Okrem priamych finančných nákladov predstavujú nové regulácie pre MSP významnú administratívnu záťaž. Táto záťaž zahŕňa požiadavky na dokumentáciu, reporting, dodržiavanie lehôt a komunikáciu s regulačnými orgánmi.

Administratívne požiadavky AI Act

Pre poskytovateľov vysokorizikových AI systémov:

- Technická dokumentácia - podrobná dokumentácia preukazujúca súlad so všetkými požiadavkami, vrátane popisu systému, účelu, údajových súborov, trénovacích metód a testovania
- Systém riadenia kvality - dokumentovaný QMS pokrývajúci celý životný cyklus AI systému
- Registrácia v databáze EÚ - povinná registrácia vysokorizikových AI systémov v celoeurópskej databáze pred uvedením na trh
- Posúdenie zhody - Vykonanie a zdokumentovanie posúdenia zhody (interné alebo treťou stranou)
- Vyhlásenie o zhode a CE označenie - Vypracovanie EÚ vyhlásenia o zhode a umiestnenie CE označenia na produkt
- Uchovávanie logov - Automatické zaznamenávanie udalostí relevantných pre identifikáciu rizík počas celého životného cyklu systému
- Monitorovanie po uvedení na trh - Aktívne sledovanie fungovania systému a hlásenie závažných incidentov

Pre nasadzovateľov vysokorizikových AI systémov:

- Hodnotenie vplyvu na základné práva - Povinné pre určité kategórie nasadzovateľov pred prvým použitím systému
- Ľudský dohľad - Zabezpečenie adekvátneho ľudského dohľadu nad vysokorizikovými AI systémami
- Uchovávanie vstupných údajov - Uchovávanie logov vstupných údajov po dobu primeranú účelu systému
- AI gramotnosť - Zabezpečenie dostatočnej úrovne AI gramotnosti zamestnancov pracujúcich s AI systémami (povinnosť účinná od 2. februára 2025)

Administratívne požiadavky CRA

Dokumentačné povinnosti výrobcov:

- Zaobstaranie technickej dokumentácie demonštrujúca splnenie základných požiadaviek na kybernetickú bezpečnosť
- SBOM (Software Bill of Materials): Detailný a prístupný zoznam všetkých komponentov produktu
- Informácie pre používateľov: Jasné a zrozumiteľné informácie o bezpečnostných vlastnostiach produktu
- Uchovávanie dokumentácie na obdobie minimálne 10 rokov po uvedení produktu na trh

Reportingové povinnosti (účinné od 11. septembra 2026):

- Hlásenie zraniteľností - aktívne zneužívané zraniteľnosti musia byť nahlásené ENISA do 24 hodín
- Hlásenie incidentov - závažné bezpečnostné incidenty ovplyvňujúce produkt musia byť nahlásené do 24 hodín
- Informovanie používateľov - používatelia musia byť informovaní o incidentoch a opatreniach na ich zmiernenie v primeranom čase
- Hlásenie zraniteľností v komponentoch - Informovanie správcov integrovaných komponentov o identifikovaných zraniteľnostiach

Administratívne požiadavky NIS2

Registračné a notifikačné povinnosti:

- Oznámenie začatia činnosti - Prevádzkovatelia základnej služby musia oznámiť NBÚ začatie činnosti do 60 dní od vzniku povinnosti
- Prvotné hlásenie incidentu - Do 24 hodín od zistenia závažného kybernetického bezpečnostného incidentu
- Podrobné hlásenie - Do 72 hodín s detailnými informáciami o incidente, jeho dopade a prijatých opatreniach
- Záverečná správa - Kompletná správa o incidente vrátane analýzy príčin do jedného mesiaca

Dokumentácia bezpečnostných opatrení (podľa § 20 zákona č. 366/2024 Z. z.):

- Dokumentácia analýzy rizík a politiky bezpečnosti informačných systémov
- Zdokumentované postupy riadenia incidentov
- Plány kontinuity podnikania a krízového riadenia
- Evidencia o hodnotení bezpečnosti dodávateľského reťazca
- Záznamy o školeniach zamestnancov v oblasti kybernetickej bezpečnosti
- Dokumentácia politík a postupov pre kryptografiu a šifrovanie

Personálne a technologické požiadavky

Implementácia nových regulačných požiadaviek si vyžaduje nielen finančné investície, ale aj adekvátne ľudské zdroje a technickú infraštruktúru. Pre MSP to často znamená potrebu prijať nových špecialistov alebo vytvoriť úplne nové pracovné pozície.

3.3.1 Požiadavky na ľudské zdroje

Nedostatok odborníkov ako kľúčová výzva: Podľa prieskumu ENISA z roku 2024 až 89 % organizácií očakáva, že bude potrebovať dodatočných zamestnancov v oblasti kybernetickej bezpečnosti na splnenie požiadaviek NIS2. Zároveň 32 % organizácií (a až 59 % MSP) hlási ťažkosti s obsadzovaním pozícií v kybernetickej bezpečnosti, najmä tých vyžadujúcich technickú expertízu. Iba 13 % MSP má v súčasnosti predplatené služby kybernetického poistenia.[10]

Nové pracovné pozície a role: V závislosti od rozsahu aktivít a typu regulácie môžu MSP potrebovať:

- AI Compliance Officer / AI Ethics Officer - zodpovedný za dohľad nad súladom AI systémov s AI Act, vrátane monitorovania, dokumentácie a komunikácie s regulačnými orgánmi
- Cybersecurity Officer / CISO - riadiaci pracovník zodpovedný za implementáciu a dohľad nad kybernetickou bezpečnosťou. NIS2 výslovne stanovuje zodpovednosť vrcholového vedenia za kybernetickú bezpečnosť
- Špecialisti na kybernetickú bezpečnosť - security analytici, penetrační testeri, správcovia bezpečnostných systémov
- Právnici so znalosťou AI a dátovej ochrany - potrební na interpretáciu regulácií a zabezpečenie právnej compliance
- Interní audítori - pre pravidelné overovanie súladu s požiadavkami regulácií

Náklady na ľudské zdroje: Priemerné ročné náklady na špecialistu v oblasti kybernetickej bezpečnosti v Európe sa pohybujú od 30 000 do 70 000 EUR pre juniorné a stredné pozície, až po 80 000 - 180 000 EUR pre seniorných expertov a manažérov. V západnej Európe (Nemecko, Holandsko, Belgicko) sú mzdy vyššie, pričom priemerný plat v kybernetickej bezpečnosti dosahuje 45 000 - 126 000 EUR v Belgicku. Pre pozíciu CISO sa platy v Európe pohybujú od 150 000 do 400 000 EUR ročne v závislosti od veľkosti organizácie a krajiny. MSP môžu alternatívne využiť externé služby - outsourcing kybernetickej bezpečnosti môže priniesť úspory 35-60 % oproti internému riešeniu.[11]

3.3.2 Technologické investície

Splnenie požiadaviek regulácií si vyžaduje investície do technickej infraštruktúry. Rozsah investícií závisí od aktuálneho stavu bezpečnostných systémov podniku a typu regulácie.

Kľúčové technologické investície pre NIS2 a CRA:

- Systémy detekcie a prevencie prienikov (IDS/IPS): Náklady 10 000 – 100 000 EUR v závislosti od komplexnosti siete

[10] ENISA. *NIS Investments 2024 Report*. European Union Agency for Cybersecurity, 2024. Dostupné na: https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf

[11] *Payscale*. **Cyber Security Salary in Belgium** (priemerné platy pre špecialistov kybernetickej bezpečnosti v Belgicku v rozsahu približne €31 000 – €147 000 ročne). Dostupné online: https://www.payscale.com/research/BE/Skill%3DCyber_Security/Salary

- SIEM/XDR riešenia: Security Information and Event Management systémy pre centralizovaný monitoring - 20 000 - 200 000 EUR ročne
- Riešenia na monitorovanie zraniteľností: Nástroje na kontinuálne skenovanie a identifikáciu bezpečnostných slabín - 5 000 - 50 000 EUR ročne
- Zálohovacie a disaster recovery riešenia: Systémy na zálohovanie dát a obnovu po havárii - 10 000 - 100 000 EUR
- Šifrovacie riešenia: Implementácia end-to-end šifrovania pre dáta v pohybe aj v pokoji
- Multi-factor autentifikácia (MFA): Povinná podľa NIS2 - náklady 2 - 10 EUR mesačne na používateľa, alebo zariadenie[12]

Technologické investície pre AI Act:

- Systémy na logging a audit trail - pre automatické zaznamenávanie aktivít AI systémov
- Nástroje na monitoring AI výstupov - pre zabezpečenie ľudského dohľadu a detekciu anomálií
- Platformy na správu dát a dátovú governance - pre zabezpečenie kvality a reprezentatívnosti trénovacích dát
- Testovacie prostredia - infraštruktúra na testovanie a validáciu AI systémov pred nasadením

3.4 Finančné náklady vs. prínosy

Hoci nové regulácie predstavujú pre MSP významné náklady, je potrebné ich hodnotiť v kontexte prínosov, ktoré compliance môže priniesť. Tieto prínosy môžu byť priame (finančné) aj nepriame (strategické, reputačné).

3.4.1 Prínosy pre MSP

Compliance s reguláciami je predpokladom pre legálne pôsobenie na európskom trhu. Pre výrobcov produktov s digitálnymi prvkami CE označenie podľa CRA signalizuje súlad s bezpečnostnými požiadavkami a umožňuje voľný pohyb tovaru v rámci EÚ. Certifikácia podľa EU Cybersecurity Act vytvára jednotný rámec uznávaný vo všetkých členských štátoch, čím sa zjednodušuje expanzia na nové trhy.

V prostredí rastúcich kybernetických hrozieb sa kybernetická bezpečnosť stáva konkurenčnou výhodou. Podľa prieskumov organizácie s robustnými bezpečnostnými opatreniami dosahujú vyššiu mieru dôvery zákazníkov a obchodných partnerov. Compliance s AI Act signalizuje zodpovedný a etický prístup k využívaniu umelej inteligencie, čo môže byť rozhodujúcim faktorom pri výbere dodávateľa najmä vo verejnom sektore a regulovaných odvetviach.[13]

[12] *ISMS.online*. *NIS 2 Compliance Costs: Overview of Compliance Investments and Hidden Fees* — detailný prehľad typov nákladov súvisiacich s technologickými investíciami pri implementácii požiadaviek NIS2 (napr. nástroje na monitoring, SIEM/XDR, MFA a ďalšie). Online dostupné: https://www.isms.online/nis-2/overview/costs/

[13] **European Commission.** *Regulation (EU) 2024/1689 – Artificial Intelligence Act.* Official Journal of the European Union, 2024. Nariadenie zavádza požiadavky na systém riadenia kvality (QMS), riadenie rizík a

Implementácia bezpečnostných opatrení požadovaných NIS2 a CRA znižuje pravdepodobnosť úspešného kybernetického útoku. Podľa IBM Cost of a Data Breach Report priemerné náklady na narušenie bezpečnosti údajov v roku 2024 dosiahli 4,88 milióna USD. Organizácie s dobre implementovanými bezpečnostnými opatreniami môžu ušetriť v priemere 10 % nákladov súvisiacich s narušením bezpečnosti. Investícia do prevencie je tak spravidla nižšia ako potenciálne náklady na riešenie bezpečnostného incidentu.[14]

Implementácia compliance programu často vedie k optimalizácii interných procesov, lepšej dokumentácii a vyššej efektivite. Zavedenie QMS požadovaného AI Act môže priniesť prínosy aj v iných oblastiach riadenia kvality. Pravidelné hodnotenie rizík a audity identifikujú slabé miesta nielen v bezpečnosti, ale aj v celkovom fungovaní organizácie.

NIS2 vyžaduje, aby regulované subjekty zabezpečili kybernetickú bezpečnosť svojho dodávateľského reťazca. MSP, ktoré preukážu súlad s reguláciami, budú preferovanými dodávateľmi pre veľké podniky a subjekty verejnej správy. Tento trend je už viditeľný - vládne zákazky čoraz častejšie vyžadujú preukázanie kybernetickej zrelosti dodávateľov.

3.4.2 Bilancia nákladov a prínosov

Celkové hodnotenie bilancie nákladov a prínosov závisí od konkrétnej situácie podniku. Pre MSP s vysokou expozíciou kybernetickým rizikám alebo pôsobiace v regulovaných sektoroch budú prínosy compliance spravidla prevyšovať náklady. Pre podniky s nízkou digitálnou intenzitou môžu byť náklady proporcionálne vyššie.

Tab. č. 1: **Porovnanie nákladov a prínosov compliance**

Náklady	Prínosy
Jednorazové investície do technológií a systémov	Prístup na jednotný trh EÚ s 450+ mil. Spotrebiteľmi
Ročné náklady na údržbu a aktualizácie	Zníženie pravdepodobnosti a dopadov kybernetických incidentov
Náklady na špecialistov a školenia	Zvýšenie dôvery zákazníkov a partnerov
Administratívna záťaž a čas manažmentu	Konkurenčná výhoda v dodávateľských reťazcoch
Náklady na certifikáciu a posúdenie zhody	Optimalizácia interných procesov
Poistenie kybernetických rizík	Vyhnutie sa pokutám (až 10 mil. EUR / 2 % obratu)

Zdroj: European Commission. *Regulation (EU) 2024/1689 – Artificial Intelligence Act.* Official Journal of the European Union, 2024., European Parliament and Council. *Directive (EU) 2022/2555 (NIS2 Directive).* Official Journal of the European Union, 2022., European Commission. *Cyber Resilience Act (Regulation (EU) 2024/2847).* Official Journal of the European Union, 2024, IBM Security. *Cost of a Data Breach Report 2024.* IBM Corporation, 2024

Priame dopady nových technologických regulácií EÚ na MSP sú významné, avšak nie rovnomerné. Najvyššie náklady budú znášať poskytovatelia vysokorizikových AI systémov

dokumentáciu pre vysokorizikové AI systémy, čo podporuje dôveru a transparentnosť pri výbere dodávateľov, najmä vo verejnom sektore

[14] **IBM Security.** *Cost of a Data Breach Report 2024.* Armonk, NY: IBM Corporation, 2024. Priemerné globálne náklady na narušenie bezpečnosti údajov dosiahli 4,88 mil. USD; organizácie s vyspelými bezpečnostnými opatreniami dosahujú nižšie náklady na incident. Dostupné online: https://www.ibm.com/reports/data-breach

a výrobcovia produktov s digitálnymi prvkami. Pre stredné podniky v regulovaných sektoroch NIS2 predstavuje NIS2 komplexnú zmenu v prístupe ku kybernetickej bezpečnosti. Regulácie však obsahujú mechanizmy na zmiernenie záťaže pre MSP - zjednodušenú dokumentáciu, znížené poplatky, prioritný prístup do sandboxov a proporcionálne sankcie. Kľúčom k úspešnému zvládnutiu regulačných zmien je včasná príprava, strategický prístup a využitie dostupných podporných nástrojov.

4 NEPRIAME DOPADY REGULÁCIÍ NA MSP

Technologické regulácie Európskej únie - AI Act, Cyber Resilience Act a smernica NIS2 - generujú nielen priame náklady na dosiahnutie a udržanie súladu, ale aj širokú škálu nepriamych dopadov, ktoré môžu v dlhodobom horizonte prevýšiť význam priamych nákladov.

4.1 Vplyv na inovačný potenciál

Vzťah medzi reguláciou a inováciami predstavuje jeden z najdiskutovanejších a najkomplexnejších aspektov v kontexte nových technologických regulácií Európskej únie. Akademická literatúra aj praktické skúsenosti z implementácie predchádzajúcich regulácií ukazujú, že tento vzťah je inherentne ambivalentný a kontextovo závislý. Regulácie môžu inovácie stimulovať aj brzdiť v závislosti od ich dizajnu, spôsobu implementácie, načasovania a konkrétnych okolností na úrovni podnikov, sektorov a trhov. Pre malé a stredné podniky je pochopenie tejto dynamiky kľúčové pre strategické rozhodovanie v období zásadných regulačných zmien.

Historicky sa vzťah medzi reguláciou a inováciami interpretoval prevažne cez prizmu tzv. Porterovej hypotézy, podľa ktorej dobre navrhnuté environmentálne regulácie môžu stimulovať inovácie, ktoré čiastočne alebo úplne kompenzujú náklady na súlad. Táto hypotéza bola následne rozšírená aj na iné typy regulácií vrátane regulácií v oblasti bezpečnosti produktov, ochrany údajov a digitálnych technológií. Empirické dôkazy však ukazujú, že platnosť tejto hypotézy závisí od mnohých faktorov vrátane veľkosti podniku, sektora, typu regulácie a spôsobu jej implementácie.

Pre slovenské MSP je kľúčové, aby nové regulácie AI Act, CRA a NIS2 neboli vnímané iba ako dodatočná administratívna a finančná záťaž, ale aj ako rámec, ktorý môže podporiť dôveru v digitálne riešenia, uľahčiť vstup na nové trhy a motivovať k systematickejšiemu prístupu k výskumu, vývoju a inováciám. Zároveň je však potrebné realisticky identifikovať riziká, ktoré komplexné regulačné požiadavky predstavujú pre inovačný potenciál menších podnikov s obmedzenými zdrojmi.

4.1.1 Teoretický rámec vzťahu regulácie a inovácií

Pred analýzou konkrétnych dopadov technologických regulácií EÚ na inovačný potenciál MSP je potrebné vymedziť teoretický rámec, ktorý umožňuje systematické pochopenie vzťahu medzi reguláciou a inováciami. Ekonomická teória ponúka niekoľko perspektív na tento vzťah, ktoré sa vzájomne dopĺňajú a poskytujú komplexnejší obraz.

Porterova hypotéza a jej modifikácie

Porterova hypotéza, formulovaná Michaelom Porterom a Classom van der Lindem v roku 1995, predstavuje jeden z najvplyvnejších teoretických rámcov pre analýzu vzťahu medzi reguláciou a konkurencieschopnosťou. Podľa tejto hypotézy prísne, ale dobre navrhnuté regulácie môžu stimulovať inovácie, ktoré nielen kompenzujú náklady na súlad, ale môžu viesť k absolútnym konkurenčným výhodám. Mechanizmus pôsobenia spočíva v tom, že regulácie signalizujú podnikom oblasti neefektívnosti a stimulujú hľadanie inovatívnych riešení, ktoré by bez regulačného tlaku neboli identifikované.[15]

Aplikácia Porterovej hypotézy na technologické regulácie EÚ naznačuje, že požiadavky AI Act, CRA a NIS2 môžu stimulovať inovácie v oblasti bezpečnosti, kvality a etiky digitálnych produktov a služieb. Podniky, ktoré úspešne integrujú tieto požiadavky do svojich produktov, môžu získať konkurenčnú výhodu na trhoch, kde zákazníci čoraz viac oceňujú bezpečnosť a dôveryhodnosť digitálnych riešení.

Teória regulačnej záťaže

Alternatívny teoretický prístup zdôrazňuje náklady regulácie a jej potenciálne brzdiace účinky na inovácie. Podľa tejto perspektívy regulácie odčerpávajú zdroje, ktoré by inak mohli byť investované do výskumu a vývoja, a vytvárajú administratívnu záťaž, ktorá spomaľuje inovačné procesy. Tento efekt je obzvlášť výrazný u menších podnikov, ktoré nemajú kapacitu na absorpciu fixných nákladov compliance a musia proporcionálne viac investovať do súladu na úkor inovácií.

Empirické štúdie o dopadoch GDPR poskytujú podporu pre túto perspektívu. Výskum ukázal, že GDPR malo merateľný negatívny dopad na ziskovosť a inovačný výstup firiem, pričom tento efekt bol výraznejší u menších spoločností. Podľa štúdie CEPR spoločnosti orientované na trhy EÚ zaznamenali v priemere 8% zníženie ziskov, pričom primárnym kanálom dopadu boli práve náklady na compliance.

Teória regulačného podnikateľstva

Tretia teoretická perspektíva vníma regulácie ako zdroj podnikateľských príležitostí. Podľa tohto prístupu regulácie vytvárajú nové trhy pre produkty a služby, ktoré pomáhajú podnikom dosiahnuť súlad. Podniky, ktoré dokážu tieto príležitosti identifikovať a využiť, môžu profitovať z regulačných zmien. Táto perspektíva je obzvlášť relevantná pre MSP pôsobiace v oblasti kybernetickej bezpečnosti, konzultačných služieb a technologických riešení.

V kontexte AI Act, CRA a NIS2 vzniká významný dopyt po špecializovaných službách a produktoch, čo predstavuje príležitosť pre MSP s príslušnou expertízou. Trh compliance

[15] PORTER, Michael E.; VAN DER LINDE, Claas. **Toward a New Conception of the Environment–Competitiveness Relationship.** *Journal of Economic Perspectives*, 1995, roč. 9, č. 4, s. 97–118.

služieb v oblasti kybernetickej bezpečnosti a AI sa očakáva, že bude výrazne rásť v nasledujúcich rokoch, čo vytvára priestor pre nové podnikateľské modely.

4.1.2 Empirické dôkazy o vplyve regulácií na inovácie

Analýza vplyvu existujúcich regulácií, najmä GDPR ako najrelevantnejšieho precedensu, poskytuje empirické dôkazy o tom, ako môžu technologické regulácie ovplyvniť inovačný potenciál podnikov. Tieto poznatky sú kľúčové pre predikciu dopadov AI Act, CRA a NIS2 a pre formuláciu odporúčaní pre MSP.

Kvantitatívne dopady GDPR na firmy

Podľa komplexnej štúdie publikovanej na platforme CEPR (Centre for Economic Policy Research) malo zavedenie GDPR merateľný negatívny dopad na ziskovosť a inovačný výstup firiem. Výskumníci analyzovali údaje z tisícov európskych spoločností a porovnali ich výkonnosť s kontrolnou skupinou firiem mimo EÚ. Kľúčové zistenia štúdie zahŕňajú 8% zníženie ziskov pre spoločnosti orientované na trhy EÚ, pomerne mierne 2% zníženie tržieb naznačujúce, že primárnym kanálom dopadu boli náklady na compliance, nie pokles dopytu a žiadny štatisticky významný dopad na veľké technologické spoločnosti (BigTech), ktoré mohli absorpovať náklady a potenciálne zvýšiť trhový podiel na úkor menších konkurentov.[16]

Osobitne zaujímavým zistením je asymetrický dopad na podniky rôznej veľkosti. Medzi malými spoločnosťami v sektore informačných technológií bol negatívny dopad na zisky dvojnásobný v porovnaní s priemerným efektom naprieč celou vzorkou. Veľké technologické spoločnosti tak podľa výskumníkov mohli využiť GDPR na posilnenie svojej trhovej pozície na úkor menších konkurentov, čím kompenzovali vlastné náklady na compliance.

Tab. č. 2: **Dopady GDPR na firmy podľa veľkosti a sektora**

Kategória firiem	Dopad na zisky	Dopad na tržby	Štatistická významnosť
Všetky firmy orientované na EÚ	-8 %	-2 %	Vysoká
Malé IT spoločnosti	-16 %	-3 %	Vysoká
Veľké technologické spoločnosti	Nevýznamný	Nevýznamný	Nízka
Stredné podniky	-6 %	-2 %	Stredná
Dátovo intenzívne sektory	-12 %	-4 %	Vysoká

Zdroj: Vlastné spracovanie podľa CEPR VoxEU, 2021; štúdia Frey & Presidente, Economic Inquiry, 2024

Náklady na compliance podľa veľkosti podniku

Štúdia Európskeho parlamentu z roku 2024 analyzovala náklady na súlad s rôznymi reguláciami v závislosti od veľkosti podniku. Výsledky jednoznačne potvrdili regresívny

[16] JIA, Jian; JIN, Ginger Zhe; WAGMAN, Liad. **The Short-Run Effects of GDPR on Technology Venture Investment.** CEPR Discussion Paper No. DP13753. Centre for Economic Policy Research, 2019.

charakter regulačnej záťaže, teda skutočnosť, že menšie podniky znášajú proporcionálne vyššie náklady.[17] Konkrétne údaje ukazujú, že náklady na compliance predstavovali 0,1 % obratu pre veľké spoločnosti, 0,3 % obratu pre stredné podniky (50 až 249 zamestnancov), 0,8 % obratu pre malé podniky (10 až 49 zamestnancov) a 1,9 % obratu pre mikropodniky (do 9 zamestnancov).[18]

Tieto údaje majú zásadné implikácie pre pochopenie dopadov na inovačný potenciál. Mikropodnik s obratom 500 000 EUR ročne vynakladá na compliance približne 9 500 EUR, čo môže predstavovať významnú časť jeho rozpočtu na výskum a vývoj. Naopak, veľký podnik s obratom 100 miliónov EUR vynakladá na compliance približne 100 000 EUR, čo je v absolútnych číslach viac, ale v proporcionálnom vyjadrení výrazne menej zaťažujúce.

Vplyv na inovačný výstup

Štúdia publikovaná v časopise Industry and Innovation (2023) skúmala priamy vplyv GDPR na produktové inovácie. Výskumníci využili kondicionálny difference-in-differences výskumný dizajn a analyzovali údaje z nemeckého inovačného prieskumu. Kľúčovým zistením bolo, že GDPR viedlo k významného posunu od radikálnych k inkrementálnym produktovým inováciám. Firmy sa primárne sústredili na reorganizáciu správy dát a zlepšovanie existujúcich produktov, nie na vývoj zásadne nových riešení.[19]

Tento posun má dlhodobé implikácie pre konkurencieschopnosť európskych firiem. Radikálne inovácie sú typicky zdrojom disruptívnych konkurenčných výhod a umožňujú firmám vstúpiť na nové trhy alebo zásadne zmeniť existujúce. Ak regulácie systematicky posúvajú inovačné úsilie smerom k inkrementálnym zlepšeniam, môže to v dlhodobom horizonte oslabiť pozíciu európskych firiem voči konkurentom z menej regulovaných regiónov.

Dopad na startupovú aktivitu

Osobitne významným indikátorom vplyvu regulácií na inovácie je ich dopad na zakladanie nových podnikov. Štúdia Jia et al. (2021) analyzovala vplyv GDPR na investície do technologických startupov a zistila pokles rizikového kapitálu smerujúceho do európskych startupov v porovnaní s americkými po zavedení GDPR. Tento efekt bol obzvlášť výrazný u startupov zameraných na dátovo intenzívne obchodné modely.[20]

---

[17] **European Parliament.** *The impact of EU legislation on SMEs – Costs and benefits.* Study requested by the Committee on Industry, Research and Energy (ITRE). Luxembourg: Publications Office of the European Union, 2024.

[18] **European Commission.** *Annual Burden Survey 2022 – Regulatory costs and administrative burden for SMEs.* Brussels: European Commission, 2023.

[19] **Blind, Knut; Niebel, Thomas; Ramel, Florian; Ziesemer, Thomas.** *The impact of the General Data Protection Regulation (GDPR) on innovation: Evidence from the German innovation survey.* **Industry and Innovation**, 2023, roč. 30, č. 8, s. 1002–1026.

[20] JIA, Jian; JIN, Ginger Zhe; WAGMAN, Liad. **The Short-Run Effects of the General Data Protection Regulation on Technology Venture Investment.** *Marketing Science*, 2021, roč. 40, č. 4, s. 662–684.

Pre slovenský startup ekosystém tieto zistenia naznačujú, že nové technologické regulácie môžu predstavovať dodatočnú bariéru pri získavaní financovania, najmä od zahraničných investorov, ktorí môžu preferovať jurisdikcie s menej komplexným regulačným prostredím. Na druhej strane, startupy, ktoré úspešne preukážu súlad s reguláciami, môžu byť atraktívnejšie pre investorov hľadajúcich príležitosti na európskom trhu.

Tab. č. 3: **Náklady na GDPR compliance podľa veľkosti podniku**

Veľkostná kategória	% z obratu	Príklad (absolútne)	Dopad na R&D rozpočet
Mikropodnik (<10 zam.)	1,9 %	9 500 EUR pri obrate 500 000 EUR	Kritický
Malý podnik (10-49 zam.)	0,8 %	16 000 EUR pri obrate 2 mil. EUR	Významný
Stredný podnik (50-249 zam.)	0,3 %	30 000 EUR pri obrate 10 mil. EUR	Mierny

Zdroj: Štúdia Európskeho parlamentu, 2024; vlastné výpočty

4.1.3 Regulačné sandboxy ako nástroj podpory inovácií

AI Act v článkoch 57 až 63 zavádza koncept regulačných sandboxov (regulatory sandboxes), ktoré predstavujú kontrolované prostredia, kde môžu organizácie vyvíjať, trénovať, testovať a validovať inovatívne AI systémy pred ich uvedením na trh. Tento nástroj je explicitne zameraný na podporu MSP a startupov a má potenciál zmierniť negatívne dopady regulácie na inovácie tým, že poskytuje bezpečné prostredie pre experimentovanie s novými technológiami.

Právny rámec regulačných sandboxov podľa AI Act

Regulačné sandboxy podľa AI Act predstavujú právne definovaný rámec, ktorý stanovuje práva a povinnosti všetkých zúčastnených strán. Článok 57 nariadenia definuje sandbox ako kontrolovaný rámec zriadený kompetentným orgánom, ktorý ponúka poskytovateľom alebo potenciálnym poskytovateľom AI systémov možnosť vyvíjať, trénovať, validovať a testovať, v prípade potreby v reálnych podmienkach, inovatívny AI systém podľa špecifického sandboxového plánu na obmedzený čas pod regulačným dohľadom.

Členské štáty EÚ majú povinnosť zriadiť aspoň jeden funkčný AI regulačný sandbox do 2. augusta 2026. Nariadenie umožňuje aj vytvorenie spoločných sandboxov viacerými členskými štátmi, čo môže byť relevantné pre menšie krajiny ako Slovensko, ktoré nemusia mať kapacitu na prevádzku plnohodnotného samostatného sandboxu. Národné kompetentné orgány poskytujú účastníkom sandboxov usmernenia, dohľad a podporu pri identifikácii rizík a zabezpečení súladu s AI Act a ďalšou relevantnou legislatívou vrátane GDPR, sektorových regulácií a pravidiel ochrany spotrebiteľa.

Prioritný prístup pre MSP a startupy

Článok 57 odsek 9 AI Act explicitne stanovuje, že MSP a startupy majú prioritný prístup do regulačných sandboxov. Toto ustanovenie reflektuje uznanie skutočnosti, že menšie podniky čelia proporcionálne vyšším nákladom na compliance a majú obmedzené kapacity na testovanie inovatívnych riešení v regulačne neistom prostredí. Prioritný prístup má

zabezpečiť, že sandboxy nebudú dominované veľkými korporáciami s väčšími zdrojmi na prípravu žiadostí a účasť v sandboxových programoch.

Podľa článku 62 odsek 5 majú MSP a startupy právo na bezplatný prístup do sandboxov, hoci národné orgány môžu vymáhať náhradu primeraných a proporcionálnych výnimočných nákladov. Toto ustanovenie je kľúčové pre zabezpečenie reálnej dostupnosti sandboxov pre menšie podniky, ktoré by inak mohli byť z dôvodu finančných bariér odradené.

Ochranné mechanizmy pre účastníkov sandboxov

Účastníci sandboxov používajú niekoľko významných ochranných mechanizmov, ktoré znižujú riziko spojené s testovaním inovatívnych technológií. Predovšetkým, podľa článku 57 odsek 12, účastníci, ktorí konajú v dobrej viere a dodržiavajú sandboxový plán a usmernenia regulátora, sú chránení pred administratívnymi pokutami za porušenie AI Act počas testovania. Táto ochrana je zásadná, pretože pokuty podľa AI Act môžu dosiahnuť až 35 miliónov EUR alebo 7 % celosvetového ročného obratu, čo by pre MSP znamenalo existenčné ohrozenie.

Ochrana pred pokutami sa však nevzťahuje na zodpovednosť za škody spôsobené tretím stranám. Účastníci sandboxov zostávajú zodpovední podľa aplikovateľných právnych predpisov o zodpovednosti za škodu. Pre MSP to znamená potrebu zabezpečiť adekvátne poistné krytie aj počas účasti v sandboxe.

Dokumentácia zo sandboxu ako dôkaz súladu

Významným prínosom účasti v sandboxe je, že dokumentácia vytvorená počas testovania môže slúžiť ako dôkaz súladu s požiadavkami AI Act v rámci následného procesu posúdenia zhody. Podľa článku 63 kompetentné orgány poskytnú účastníkom, ktorí úspešne ukončia testovanie, písomné potvrdenie o aktivitách vykonaných v sandboxe a súvisiacich výsledkoch. Tento exit report môže výrazne znížiť náklady a čas potrebný na formálne posúdenie zhody a uvedenie produktu na trh.

Pre MSP, ktoré vyvíjajú vysokorizikové AI systémy podliehajúce požiadavkám podľa článku 6 AI Act, môže byť účasť v sandboxe nákladovo efektívnym spôsobom, ako prejsť časťou compliance procesu pod dohľadom regulátora a s jeho spätnou väzbou. Alternatívou by bolo vykonanie compliance aktivít samostatne s rizikom, že finálne posúdenie zhody odhalí nedostatky vyžadujúce nákladné opravy.

Tab. č. 4: **Kľúčové ustanovenia AI Act o regulačných sandboxoch**

Článok	Obsah ustanovenia	Význam pre MSP
Čl. 57	Definícia a účel sandboxov, povinnosť členských štátov zriadiť aspoň jeden sandbox do augusta 2026	Garantovaná dostupnosť sandboxu v každom členskom štáte alebo cezhraničný prístup
Čl. 57(9)	Prioritný prístup pre MSP a startupy	Prednostné posudzovanie žiadostí MSP, vyššia šanca na prijatie
Čl. 57(12)	Ochrana pred pokutami pri konaní v dobrej viere	Zníženie rizika pri experimentovaní s novými technológiami
Čl. 62(5)	Bezplatný prístup pre MSP a startupy	Odstránenie finančnej bariéry účasti
Čl. 63	Dokumentácia a exit report ako dôkaz súladu	Zníženie nákladov na následné posúdenie zhody

Zdroj: Nariadenie (EÚ) 2024/1689 (AI Act)

Skúsenosti z existujúcich sandboxov

Koncept regulačných sandboxov nie je nový a existujú bohaté skúsenosti z ich implementácie v iných sektoroch, najmä vo finančných službách. Tieto skúsenosti poskytujú cenné poznatky o potenciálnych prínosoch a limitáciách sandboxov pre podporu inovácií.

Fintech sandbox britského regulátora FCA (Financial Conduct Authority), spustený v roku 2016, predstavuje jeden z najlepšie zdokumentovaných a najúspešnejších príkladov. Do roku 2023 prešlo sandboxom viac ako 800 firiem, z ktorých väčšinu tvorili startupy a MSP. Štúdie o dopadoch FCA sandboxu preukázali niekoľko významných prínosov. Spoločnosti, ktoré úspešne absolvovali testovanie v sandboxe, získali v priemere 6,6-krát viac investícií od fintech investorov v porovnaní s konkurentmi, ktorí sandbox nevyužili. Miera prežitia firiem, ktoré prešli sandboxom, bola výrazne vyššia ako u porovnateľných firiem mimo sandboxu. Účastníci sandboxu mali kratší čas uvedenia produktu na trh (time-to-market) v dôsledku včasného vyjasnenia regulačných požiadaviek.[21]

Španielsko bolo prvým členským štátom EÚ, ktorý spustil AI regulačný sandbox, a to už v roku 2022, teda pred nadobudnutím účinnosti AI Act. Španielsky sandbox AESIA (Agencia Española de Supervisión de la Inteligencia Artificial) poskytuje praktické skúsenosti s testovaním AI systémov v európskom regulačnom kontexte. Prvé kohorty účastníkov zahŕňali projekty v oblasti zdravotníctva, finančných služieb a verejnej správy, čo naznačuje široký záujem o využitie sandboxov naprieč sektormi.

Iniciatíva EUSAiR a európska koordinácia

Európska komisia v spolupráci s AI Office spustila projekt EUSAiR (EU Regulatory Sandboxes for AI), financovaný z programu Digitálna Európa. Tento dvojročný projekt má za cieľ podporiť implementáciu AI regulačných sandboxov naprieč členskými štátmi

[21] CORBETT, Jonathan; LEHTONEN, Jukka; PEARSON, Simon; et al. **The Impact and Effectiveness of Innovate UK and FCA Regulatory Sandboxes.** London: Financial Conduct Authority (FCA), 2021.

prostredníctvom vypracovania spoločných rámcov, posilnenia technických a právnych kapacít a podpory spolupráce a výmeny skúseností.

Projekt EUSAiR je vedený Talianskym výskumným centrom pre vysokovýkonné počítanie, veľké dáta a kvantové počítanie (CINECA) a združuje popredné európske univerzity, superpočítačové centrá, siete digitálnych MSP a expertov na governance AI. Konzorcium zahŕňa organizácie ako European DIGITAL SME Alliance, čo zabezpečuje, že perspektívy a potreby MSP sú integrované do vývoja sandboxových rámcov od začiatku.

Pre slovenské MSP je relevantné, že projekt EUSAiR má za cieľ vytvoriť spoločné štandardy a metodiky, ktoré uľahčia cezhraničný prístup do sandboxov. MSP zo Slovenska tak nebudú odkázané výlučne na národný sandbox, ale budú môcť potenciálne využiť sandboxy v iných členských štátoch, ak budú ponúkať relevantnejšiu sektorovú expertízu alebo infraštruktúru.

4.1.4 Európske centrá digitálnych inovácií (EDIH)

Významným podporným nástrojom pre MSP v oblasti digitálnej transformácie a inovácií sú Európske centrá digitálnych inovácií (European Digital Innovation Hubs – EDIHs). Tieto centrá predstavujú kľúčovú infraštruktúru EÚ pre podporu digitalizácie MSP a verejného sektora a zohrávajú čoraz dôležitejšiu úlohu aj v kontexte implementácie nových technologických regulácií.

Koncepcia a ciele siete EDIH

Sieť EDIH bola vytvorená v rámci programu Digitálna Európa ako jedna z hlavných iniciatív na podporu digitálnej transformácie európskej ekonomiky. EDIH fungujú ako regionálne jednotné kontaktné miesta (one-stop shops), ktoré pomáhajú podnikom a organizáciám verejného sektora reagovať na digitálne výzvy a zvyšovať ich konkurencieschopnosť. Centrá kombinujú výhody regionálnej prítomnosti s príležitosťami dostupnými prostredníctvom celoeurópskej siete.

Regionálna prítomnosť EDIH im umožňuje poskytovať služby prispôsobené potrebám lokálnych podnikov, v lokálnom jazyku a v kontexte lokálneho inovačného ekosystému. Zároveň európske pokrytie siete uľahčuje výmenu najlepších praktík medzi hubmi v rôznych krajinách a poskytovanie špecializovaných služieb naprieč regiónmi, ak potrebné zručnosti nie sú lokálne dostupné.

Aktuálny stav a dosah siete EDIH

Podľa najnovších údajov Európskej komisie z mája 2025 sieť EDIH dosiahla významný rozsah a merateľný dopad. K tomuto dátumu fungovalo 168 hubov financovaných z programu Digitálna Európa, pochádzajúcich zo všetkých členských štátov EÚ a pridružených krajín vrátane Albánska, Islandu, Kosova, Lichtenštajnska, Čiernej Hory, Severného Macedónska, Nórska, Srbska, Turecka a Ukrajiny. Sieť pokrýva takmer 90 % európskych regiónov.

Z hľadiska aktivít a dosahu sieť EDIH poskytla k máju 2025 viac ako 44 000 služieb, pričom 87 % tejto podpory smeruje k MSP a zvyšných 13 % k organizáciám verejného sektora. Bolo vykonaných takmer 16 000 hodnotení digitálnej zrelosti pomocou nástroja Digital

Maturity Assessment Tool (DMAT), z toho viac ako 14 500 pre MSP. Prostredníctvom približne 5 000 podujatí bolo oslovených viac ako 200 000 účastníkov a spoločností.

Merateľný dopad na digitálnu zrelosť

Údaje o dopade siete EDIH poskytujú presvedčivé dôkazy o účinnosti tohto nástroja. Podľa správy EDIH Network Report približne 90 % firiem vykazuje zvýšenie úrovne digitálnej zrelosti po intervenciách EDIH. Najvýznamnejšie relatívne prínosy boli zaznamenané v oblasti adopcie AI a automatizácie, kde priemerné skóre digitálnej zrelosti vzrástlo až o 35 %.

Správa tiež poskytuje strategické poznatky o tom, ako firmy napredujú v digitálnej transformácii. Potvrdzuje, že digitálna obchodná stratégia je kľúčovým faktorom v počiatočných fázach procesu, nasledovaná rastom v oblasti správy dát, human-centric dizajnu a na vyšších úrovniach zrelosti adopciou AI. Tieto poznatky sú relevantné pre MSP pri plánovaní vlastnej digitalizačnej cesty.[22]

Tab. č. 5: **Kľúčové štatistiky siete EDIH (stav k máju 2025)**

Ukazovateľ	Hodnota
Počet fungujúcich hubov	168
Pokrytie európskych regiónov	Takmer 90 %
Celkový počet poskytnutých služieb	Viac ako 44 000
Podiel služieb pre MSP	87 %
Počet hodnotení digitálnej zrelosti (DMAT)	Takmer 16 000
Počet oslovených účastníkov cez podujatia	Viac ako 200 000
Firmy so zvýšenou digitálnou zrelosťou	Približne 90 %
Nárast skóre v oblasti AI a automatizácie	Až 35 %

Zdroj: EDIH Network Report, Európska komisia, máj 2025

Štyri typy služieb EDIH

EDIH poskytujú štyri základné typy služieb, ktoré sú štruktúrované tak, aby pokrývali celý životný cyklus digitálnej transformácie MSP.

- Test Before Invest (testovanie pred investíciou) predstavuje 25 % všetkých poskytnutých služieb. Táto služba umožňuje MSP prístup k technickej expertíze a experimentovaniu vrátane služieb súvisiacich s AI. Podniky majú možnosť otestovať technológie, vrátane ich environmentálneho dopadu, pred väčšími investíciami. Pre MSP zvažujúce implementáciu AI riešení je táto služba obzvlášť cenná, pretože umožňuje overiť technickú realizovateľnosť a obchodný prínos pred vynaložením významných investícií.

[22] **European Commission.** *European Digital Innovation Hubs (EDIH) Network Report 2023.*

- Školenia a rozvoj zručností tvoria 30 % aktivít EDIH. Tieto služby zahŕňajú tréningové programy pre MSP a verejný sektor zamerané na rekvalifikáciu a rozvoj pracovnej sily v oblastiach AI, kybernetickej bezpečnosti a ďalších digitálnych technológií. V kontexte AI Act, ktorý zavádza požiadavku AI gramotnosti (článok 4), sú tieto školenia obzvlášť relevantné.

- Podpora pri získavaní financovania (17 %) poskytuje poradenstvo v oblasti verejných a súkromných zdrojov financovania, prepojenie na investorov a vhodné grantové schémy. Pre MSP, ktoré potrebujú financovať investície do compliance, môže byť táto služba kľúčová pri identifikácii dostupných zdrojov podpory.

- Inovačný ekosystém a networking (27 %) buduje prepojenia s AI továrňami, zariadeniami na testovanie a experimentovanie (TEFs), ďalšími EDIH a relevantnými stakeholdermi v regiónoch a sektoroch. Tieto prepojenia môžu byť pre MSP cenné pri hľadaní partnerov, zákazníkov alebo dodávateľov v oblasti digitálnych technológií.

Nová úloha EDIH ako AI helpdeskov

V októbri 2025 Európska komisia oznámila dodatočné financovanie pre 83 EDIH s cieľom konsolidovať sieť a rozšíriť jej kapacity v oblasti podpory implementácie AI Act. V tejto novej fáze budú EDIH slúžiť ako prvá línia AI helpdeskov, čo predstavuje významnú evolúciu ich mandátu.

EDIH ako AI helpdesky budú MSP a organizáciám verejného sektora poskytovať usmernenia pri testovaní a nasadzovaní AI riešení, ponúkať poradenstvo týkajúce sa súladu s AI Act vrátane klasifikácie AI systémov podľa rizikovosti a identifikácie aplikovateľných požiadaviek, prepájať MSP so špecializovanou expertízou dostupnou v európskom inovačnom ekosystéme AI a facilitovať prístup do regulačných sandboxov a TEFs.

Táto rozšírená úloha je súčasťou širšej stratégie Apply AI Strategy a AI Continent Action Plan, ktoré majú za cieľ urýchliť adopciu AI v európskej ekonomike pri súčasnom zabezpečení súladu s regulačnými požiadavkami. Pre slovenské MSP to znamená, že budú mať k dispozícii lokálny kontaktný bod pre otázky súvisiace s AI Act a jeho praktickou implementáciou.

EDIH na Slovensku

Na Slovensku pôsobia EDIH, ktoré poskytujú služby slovenským MSP v oblasti digitálnej transformácie. Slovenské EDIH sú súčasťou celoeurópskej siete a môžu sprostredkovať prístup k expertíze a infraštruktúre dostupnej v iných členských štátoch. Pre MSP na Slovensku je kľúčové poznať dostupné EDIH, ich špecializáciu a ponúkané služby.

Využitie služieb EDIH je pre MSP bezplatné alebo vysoko dotované, čo odstraňuje finančnú bariéru prístupu k špičkovej expertíze a technológiám. MSP, ktoré aktívne využívajú služby EDIH, môžu získať konkurenčnú výhodu prostredníctvom rýchlejšej digitálnej transformácie, lepšej pripravenosti na regulačné požiadavky a prístupu k európskej inovačnej sieti.

4.1.5 Zariadenia pre testovanie a experimentovanie (TEFs)

Okrem regulačných sandboxov a EDIH zriadila EÚ sieť špecializovaných zariadení pre testovanie a experimentovanie (Testing and Experimentation Facilities – TEFs). Tieto zariadenia poskytujú fyzickú infraštruktúru a sektorovú expertízu pre praktické overenie AI a iných digitálnych technológií v reálnych podmienkach. TEFs dopĺňajú sandboxy a EDIH tým, že umožňujú testovanie v špecifických aplikačných doménach s prístupom k relevantným dátam, vybaveniu a odborníkom.

Financovanie a rozsah TEFs

Projekty TEFs získali viac ako 220 miliónov EUR v kombinovanom financovaní od Európskej komisie a členských štátov na päťročné obdobie. Tieto prostriedky sú investované do budovania špičkovej infraštruktúry, ktorá by pre individuálne MSP bola finančne nedostupná. Veľkosť investície reflektuje ambíciu vytvoriť svetovo konkurencieschopné testovacie zariadenia, ktoré pritiahnu inovátorov z celej Európy aj mimo nej.

TEFs sú navrhnuté ako zdieľané zariadenia, ktoré môžu využívať podniky všetkých veľkostí, výskumné inštitúcie a verejný sektor. Model zdieľaného prístupu umožňuje MSP využívať infraštruktúru, ktorá by inak bola dostupná len veľkým korporáciám alebo výskumným ústavom. To môže vyrovnávať konkurenčné podmienky a umožniť MSP konkurovať na báze kvality inovácií, nie veľkosti rozpočtu.

Sektorové zameranie TEFs

- TEFs pokrývajú kľúčové sektory, kde má AI najväčší transformačný potenciál. Sektorová špecializácia umožňuje hĺbkovú expertízu a prístup k doménovým dátam a infraštruktúre, ktoré by boli ťažko replikovateľné v generických testovacích prostrediach.

- TEFs pre zdravotníctvo umožňujú testovanie AI diagnostických nástrojov, systémov na podporu klinického rozhodovania a personalizovanej medicíny v kontrolovaných podmienkach s prístupom k reálnym zdravotníckym dátam (pri zachovaní ochrany súkromia). Pre MSP vyvíjajúce zdravotnícke AI riešenia poskytujú TEFs možnosť validácie v klinickom prostredí, čo je kritické pre získanie regulačného schválenia a dôvery zdravotníckych zariadení.

- TEFs pre výrobu sa zameriavajú na Industry 4.0 riešenia vrátane prediktívnej údržby, optimalizácie výrobných procesov, kontroly kvality pomocou AI a robotiky. Tieto zariadenia typicky disponujú demonštračnými výrobnými linkami, kde možno testovať AI riešenia bez narušenia reálnej produkcie. Pre slovenské MSP v dodávateľských reťazcoch automobilového priemyslu môžu byť tieto TEFs obzvlášť relevantné.

- TEFs pre poľnohospodárstvo poskytujú testovanie precíznych poľnohospodárskych technológií, dronov s AI pre monitoring plodín, prediktívnych systémov pre manažment fariem a riešení pre automatizáciu poľnohospodárskych procesov.

Tieto zariadenia typicky zahŕňajú skúšobné pozemky a prístup k historickým agronomickým dátam.

- TEFs pre smart cities a mobilitu umožňujú testovanie riešení pre inteligentnú dopravu, autonómne vozidlá, smart grid a ďalšie aplikácie v urbánnom prostredí. Niektoré TEFs disponujú uzavretými testovacími areálmi pre autonómne vozidlá alebo prístupom k infraštruktúre smart cities.

Prepojenie TEFs s regulačnými sandboxmi

AI Act v článku 58 odsek 3 explicitne stanovuje, že potenciálni poskytovatelia v regulačných sandboxoch, najmä MSP a startupy, majú byť nasmerovaní na relevantné služby s pridanou hodnotou vrátane TEFs a EDIH. Toto prepojenie je dôležité, pretože regulačné sandboxy sú primárne zamerané na právne a compliance aspekty, zatiaľ čo TEFs poskytujú technickú infraštruktúru pre praktické testovanie.

V praxi to znamená, že MSP vyvíjajúce inovatívny AI systém môže využiť kombináciu všetkých troch nástrojov. TEFs pre technické testovanie a validáciu v reálnych podmienkach, EDIH pre školenia, poradenstvo a networking a regulačný sandbox pre vyjasnenie regulačných požiadaviek a získanie dokumentácie preukazujúcej súlad. Tento integrovaný prístup môže výrazne znížiť riziko a náklady spojené s uvádzaním inovatívnych AI produktov na trh.

4.1.6 Potenciálne riziká brzdenia inovácií

Napriek existencii podporných mechanizmov existujú oprávnené obavy, že komplexné regulačné požiadavky môžu mať na inovácie brzdiaci účinok, najmä pre MSP s obmedzenými zdrojmi. Tieto riziká je potrebné identifikovať, pochopiť a aktívne riadiť, aby sa minimalizovali negatívne dopady na inovačný ekosystém.

Odčerpávanie zdrojov z výskumu a vývoja

Ako ukázali empirické štúdie o dopadoch GDPR, náklady na compliance môžu významne odčerpať zdroje, ktoré by inak smerovali do výskumu a vývoja. Pre MSP s obmedzenými rozpočtami môže byť potreba financovať právne poradenstvo, odborné audity, úpravy produktov a školenia zamestnancov v krátkom časovom horizonte kritická.

Podľa štúdie MIT Sloan z roku 2024 GDPR efektívne funguje ako 25% dan na menšie spoločnosti v podobe zvýšených nákladov na prácu s dátami. Najvyššie náklady znášali dátovo intenzívne sektory vrátane softvérového priemyslu (24% nárast nákladov), výroby (18%) a služieb (18%). Extrapolácia týchto údajov na AI Act a CRA naznačuje, že MSP vyvíjajúce AI riešenia alebo produkty s digitálnymi prvkami budú čeliť podobnej alebo vyššej záťaži.[23]

Pre MSP s typickým R&D rozpočtom 5 až 10 % obratu môže regulačná záťaž predstavujúca 1 až 2 % obratu znamenať zníženie inovačných kapacít o 10 až 40%. Tento efekt

[23] https://mitsloan.mit.edu/ideas-made-to-matter/gdpr-reduced-firms-data-and-computation-use

je obzvlášť problematický v kontexte globálnej konkurencie, kde firmy z menej regulovaných jurisdikcií môžu investovať väčší podiel zdrojov do inovácií.

Regulačná neistota a oneskorené usmernenia

Príliš preskriptívne alebo rýchlo sa meniace regulácie môžu vytvárať neistotu, ktorá sťažuje podnikom plánovanie a investovanie do dlhodobých projektov. Táto neistota môže brzdiť inovácie, pretože podniky sa môžu zdráhať vyčleniť zdroje na nové projekty, kým nie sú jasné finálne pravidlá a praktický výklad.

V prípade AI Act bola kritika zo strany startup komunity zameraná práve na neskorý príchod praktických usmernení. Kódex praxe pre modely všeobecného účelu (GPAI) bol publikovaný až v júli 2025, len niekoľko týždňov pred nadobudnutím účinnosti príslušných povinností 2. augusta 2025. Pre zakladateľov, ktorí musia plánovať nábor, získavanie dát a technické roadmapy mesiace vopred, takéto medzery majú reálne dôsledky na schopnosť plánovať a riadiť inovácie.

V polovici roku 2025 podpísalo viac ako tridsať zakladateľov a rizikových investorov vrátane zakladateľov popredných európskych AI spoločností otvorený list, v ktorom argumentovali, že AI Act riskuje - vytvorenie fragmentovaného, nepredvídateľného regulačného prostredia, ktoré podkope inovácie, odradí investície a v konečnom dôsledku zanechá Európu pozadu. List vyzval tvorcov politík, aby zastavili hodiny a neprinášali určité povinnosti do účinnosti, kým nebudú k dispozícii praktické compliance nástroje.

Koncentrácia trhu a vytláčanie menších hráčov

Empirické dôkazy z implementácie GDPR ukazujú, že veľké spoločnosti môžu využiť regulačné zmeny na posilnenie svojej trhovej pozície na úkor menších konkurentov. Štúdia publikovaná v Journal of Industrial Economics zistila, že GDPR viedlo k 17 % nárastu koncentrácie na trhu webových služieb, pričom veľkí hráči získali podiel na úkor menších.

Tento efekt vyplýva z niekoľkých faktorov. Veľké spoločnosti majú špecializované právne a compliance tímy, ktoré môžu efektívnejšie spracovať regulačné požiadavky. Fixné náklady na compliance sú rozložené na väčší objem produkcie, čo znižuje náklady na jednotku. Veľké spoločnosti majú lepší prístup k externému poradenstvu a technológiám. V neposlednom rade veľké spoločnosti môžu využiť regulácie ako bariéru vstupu pre nových konkurentov.

Pre MSP to znamená riziko, že AI Act, CRA a NIS2 môžu posilniť pozíciu veľkých technologických spoločností na úkor menších inovátorov. Zmierňovanie tohto rizika vyžaduje aktívnu podporu MSP zo strany verejných politík a využitie dostupných podporných nástrojov.

Nedostatočná diferenciácia požiadaviek

Podľa Gabrieleho Mazziniho, hlavného architekta AI Act, nebolo možné úplne rozlíšiť požiadavky pre menších a väčších hráčov bez rizika podkopania cieľov regulácie. V rozhovore pre IESE Insight v roku 2024 uviedol, že hoci AI Act obsahuje určité úľavy pre MSP, regulačné požiadavky môžu stále predstavovať značnú záťaž najmä pre menšie podniky, ktoré nemajú potrebné zdroje na ich implementáciu.

Táto skutočnosť podčiarkuje potrebu externej podpory a zjednodušených metodík pre menšie podniky. Bez adekvátnej podpory hrozí, že MSP budú buď nedostatočne pripravené na regulačné požiadavky, čo ich vystaví riziku sankcií a straty trhových príležitostí, alebo budú musieť vynaložiť neprimeranú časť svojich zdrojov na compliance na úkor inovácií.

Tab. č. 6: **Komplexný prehľad stimulujúcich a brzdiacich faktorov**

Stimulujúce faktory	Brzdiace faktory
Regulačné sandboxy s prioritným prístupom a ochranou pred pokutami pre MSP	Vysoké náklady na compliance (1–2 % obratu) odčerpávajúce R&D zdroje
Sieť 168 EDIH poskytujúcich bezplatné testovanie, školenia a poradenstvo	Administratívna záťaž a komplexná technická dokumentácia
TEFs s investíciou 220+ mil. EUR pre sektorové testovanie	Regulačná neistota z oneskorených usmernení a výkladov
Jasný harmonizovaný právny rámec nahradzujúci 27 národných prístupov	Nedostatok kvalifikovaných odborníkov (3,4 mil. globálny deficit v kyber)
Tlak na inovácie v bezpečnosti vytvárajúci nové trhové segmenty	Kultúra averzie voči riziku v európskom podnikateľskom prostredí
Financovanie z Horizont Europe, Digital Europe a národných programov	Pretrvávajúca fragmentácia v implementácii medzi členskými štátmi
Dôvera spotrebiteľov v regulované produkty ako konkurenčná výhoda	Posun od radikálnych k inkrementálnym inováciám
Bruselský efekt vytvárajúci globálnu relevanciu EÚ compliance	Koncentrácia trhu a vytláčanie menších hráčov

Zdroj: Vlastné spracovanie na základe štúdií CEPR, MIT Sloan, dokumentov EK a analýzy AI Act

4.1.7 Zhrnutie a odporúčania pre MSP

Vplyv technologických regulácií EÚ na inovačný potenciál MSP je komplexný a závisí od mnohých faktorov vrátane veľkosti podniku, sektora, typu inovačných aktivít a schopnosti využiť dostupné podporné nástroje. Na základe analýzy teoretického rámca, empirických dôkazov a podporných mechanizmov možno formulovať niekoľko kľúčových záverov a odporúčaní.

Kľúčové zistenia

Regulácie AI Act, CRA a NIS2 budú mať merateľný dopad na náklady MSP, pričom na základe skúseností s GDPR možno očakávať proporcionálne vyššiu záťaž pre menšie podniky. Náklady na compliance v rozsahu 0,8 až 1,9 % obratu pre malé a mikropodniky môžu významne konkurovať výdavkom na výskum a vývoj.

EÚ vytvorila robustnú infraštruktúru podpory inovácií vrátane regulačných sandboxov, siete EDIH a TEFs. Tieto nástroje poskytujú MSP prístup k expertíze, infraštruktúre a regulačnému poradenstvu, ktoré by inak neboli dostupné. Využitie týchto nástrojov môže významne zmierniť negatívne dopady regulácií.

Empirické dôkazy z implementácie GDPR ukazujú riziko koncentrácie trhu a vytláčania menších hráčov. Aktívna politika podpory MSP a využitie dostupných nástrojov sú kľúčové pre zabránenie tomuto efektu v kontexte nových technologických regulácií.

Odporúčania pre MSP

Pre slovenské MSP možno formulovať nasledovné odporúčania na maximalizáciu inovačného potenciálu v novom regulačnom prostredí.

- Prvým odporúčaním je aktívne využívanie podporných nástrojov EÚ. MSP by mali systematicky využívať služby EDIH, zvažovať účasť v regulačných sandboxoch a TEFs a sledovať dostupné grantové schémy. Tieto nástroje sú navrhnuté práve pre podporu MSP a ich nevyužitie znamená zbytočnú konkurenčnú nevýhodu.

- Druhým odporúčaním je včasná príprava na regulačné požiadavky. Namiesto čakania na finálne termíny by MSP mali začať s prípravou na compliance čo najskôr. Včasná príprava umožňuje rozložiť náklady v čase, identifikovať synergies medzi compliance a existujúcimi procesmi a vyhnúť sa nákladným opravám na poslednú chvíľu.

- Tretím odporúčaním je integrácia compliance do inovačnej stratégie. Namiesto vnímania compliance ako oddelené nákladovej položky by MSP mali hľadať spôsoby, ako compliance požiadavky integrovať do svojich produktov a služieb ako diferenciačný faktor. Bezpečnosť, transparentnosť a etika sa stávajú hodnotou, ktorú zákazníci oceňujú.

- Štvrtým odporúčaním je budovanie partnerstiev a využívanie zdieľaných zdrojov. MSP môžu znížiť náklady na compliance prostredníctvom spolupráce s inými podnikmi, účasti v sektorových iniciatívach a využívania zdieľaných služieb. Profesijné združenia a obchodné komory môžu zohrávať dôležitú úlohu pri sprostredkovaní takejto spolupráce.

- Piatym odporúčaním je investícia do kompetencií. Dlhodobá konkurencieschopnosť MSP závisí od interných kompetencií v oblasti AI, kybernetickej bezpečnosti a compliance. Investície do školení zamestnancov a prípadne do špecializovaných pozícií sa môžu vrátiť v podobe nižších externých nákladov a lepšej pripravenosti na budúce regulačné zmeny.

- Pre slovenské MSP bude kľúčové, aby mali prístup k zrozumiteľným metodikám, vzorovým dokumentom a praktickým príkladom, ktoré im umožnia minimalizovať negatívny vplyv brzdiacich faktorov a maximalizovať využitie stimulujúcich faktorov. Organizácie ako Slovak Business Agency môžu zohrávať dôležitú úlohu pri sprostredkovaní týchto informácií a podporných nástrojov slovenským MSP.

4.2 Prístup na trhy a obchodné príležitosti

Technologické regulácie Európskej únie, najmä AI Act, Cyber Resilience Act a smernica NIS2, vytvárajú nielen nové povinnosti, ale aj významné trhové príležitosti pre malé a stredné podniky. Harmonizácia regulačného rámca naprieč 27 členskými štátmi odstraňuje

fragmentáciu, ktorá historicky predstavovala jednu z najvýznamnejších bariér pre cezhraničné podnikanie. Súčasne regulácie generujú dopyt po nových produktoch a službách v oblasti compliance, kybernetickej bezpečnosti a dôveryhodnej umelej inteligencie, čo otvára priestor pre inovatívne MSP s relevantnou expertízou.

Pre slovenské MSP je pochopenie týchto trhových dynamík kľúčové pre strategické rozhodovanie. Podniky, ktoré dokážu včas identifikovať a využiť nové príležitosti, môžu získať významnú konkurenčnú výhodu. Naopak, podniky, ktoré budú regulácie vnímať výlučne ako záťaž, riskujú, že zostanú pozadu za konkurentmi, ktorí regulačnú zmenu transformujú na obchodnú príležitosť.

Táto podkapitola analyzuje výhody harmonizovaného regulačného rámca, identifikuje konkrétne trhové príležitosti pre MSP, skúma fenomén Bruselského efektu a jeho implikácie pre globálnu konkurencieschopnosť a zároveň kriticky hodnotí pretrvávajúce bariéry a výzvy, ktorým MSP čelia pri využívaní nových trhových príležitostí.

4.2.1 Výhody harmonizovaného regulačného rámca

Pred prijatím AI Act, CRA a modernizovania NIS smernice existovala v Európskej únii významná regulačná fragmentácia v oblasti digitálnych technológií a kybernetickej bezpečnosti. Jednotlivé členské štáty pristupovali k regulácii AI systémov, bezpečnosti produktov s digitálnymi prvkami a ochrany kritickej infraštruktúry rôznorodo, čo vytvára komplexné prostredie pre podniky pôsobiace na viacerých národných trhoch. Nové regulácie prinášajú jednotný rámec, ktorý nahrádza túto mozaiku národných prístupov.

Historická fragmentácia a jej náklady

Pred harmonizáciou museli podniky, ktoré chceli pôsobiť na viacerých európskych trhoch, analyzovať a dodržiavať rôzne národné požiadavky, čo generovalo významné náklady. Podľa prieskumu Eurobarometra z roku 2023 až 42% offline maloobchodníkov a 46% online maloobchodníkov uviedlo, že náklady na súlad s rôznymi národnými pravidlami predstavujú významnú bariéru pre cezhraničný predaj. Tieto náklady zahŕňali právne analýzy rôznych jurisdikcií, úpravy produktov a dokumentácie pre jednotlivé trhy, viacnásobné certifikačné procesy a monitoring zmien v legislatívach viacerých krajín.[24]

Pre MSP boli tieto náklady obzvlášť zaťažujúce, pretože fixné náklady na regulačnú analýzu a prispôsobenie sa nedali rozložiť na veľký objem predaja ako v prípade nadnárodných korporácií. Výsledkom bolo, že mnohé MSP obmedzili svoje aktivity na domáci trh alebo na malý počet susedných krajín, čím prišli o príležitosti na širšom európskom trhu.

Princíp jedného posúdenia zhody

AI Act a CRA zavádzajú princíp, podľa ktorého produkt, ktorý bol posúdený ako vyhovujúci požiadavkám v jednom členskom štáte, môže byť uvedený na trh v celej

[24] **European Commission.** *Flash Eurobarometer 531 – SMEs, cross-border trade and regulatory barriers.* Brussels: European Commission, 2023.

Európskej únii bez ďalšieho posudzovania. Tento princíp, známy z iných oblastí harmonizácie (napríklad CE označenie pre výrobky), významne znižuje transakčné náklady cezhraničného obchodu.

Pre vysokorizikové AI systémy podľa AI Act to znamená, že poskytovatelia musia prejsť procesom posúdenia zhody len raz, pričom výsledné CE označenie je platné v celej EÚ. Podobne CRA zavádza jednotné požiadavky na kybernetickú bezpečnosť produktov s digitálnymi prvkami, ktoré nahrádzajú rôzne národné prístupy. Výrobca, ktorý dosiahne súlad s CRA, môže svoj produkt predávať v ktoromkoľvek členskom štáte bez ďalších regulačných prekážok.

Tab. č. 7: **Porovnanie fragmentovaného a harmonizovaného regulačného prostredia**

Aspekt	Fragmentované prostredie (pred)	Harmonizované prostredie (po)
Právna analýza	Potrebná pre každý členský štát samostatne	Jednotný rámec pre celú EÚ
Posúdenie zhody	Viacnásobné certifikácie podľa národných požiadaviek	Jedno posúdenie platné v celej EÚ
Dokumentácia	Rôzne formáty a požiadavky podľa krajiny	Štandardizovaná dokumentácia
Monitoring legislatívy	Sledovanie zmien v 27 jurisdikciách	Sledovanie jednotného rámca EÚ
Náklady na vstup	Vysoké fixné náklady pre každý nový trh	Jednorazové náklady pre prístup na celý trh EÚ
Výhoda pre veľké firmy	Výrazná – schopnosť absorbovať náklady	Zmenšená – rovnaké pravidlá pre všetkých

Zdroj: Vlastné spracovanie na základe analyzovanej legislatívy a prieskumov Eurobarometra

Harmonizované normy a predpoklad zhody

Významným prvkom harmonizovaného rámca je systém harmonizovaných noriem, vypracovaných európskymi normalizačnými organizáciami (CEN, CENELEC, ETSI) na základe mandátu Európskej komisie. Produkty a systémy, ktoré vyhovujú tým harmonizovaným normám, ktoré boli uverejnené v Úradnom vestníku EÚ, používajú takzvaný predpoklad zhody s príslušnými požiadavkami regulácií.

Pre MSP to znamená významné zjednodušenie procesu dokazovania súladu. Namiesto individuálneho preukazovania splnenia každej regulačnej požiadavky môže podnik jednoducho deklarovať zhodu s relevantnou harmonizovanou normou. Tým sa znižujú náklady na právnu analýzu, technickú dokumentáciu a prípadné externé audity. Harmonizované normy tiež poskytujú jasné technické špecifikácie, ktoré uľahčujú navrhovanie produktov a systémov od začiatku v súlade s požiadavkami.

K novembru 2025 Európska komisia intenzívne pracuje na mandátoch pre harmonizované normy k AI Act a CRA. Prvé harmonizované normy pre AI Act sa očakávajú v priebehu roku 2026, pričom prioritu majú normy pre vysokorizikové systémy v oblastiach ako biometrická identifikácia, kritická infraštruktúra a prístupy k základným službám.

Kvantifikácia prínosov harmonizácie

Ekonomické štúdie kvantifikujú prínosy regulačnej harmonizácie v rôznych oblastiach. Podľa analýzy Európskej komisie k návrhu CRA môže harmonizácia požiadaviek na kybernetickú bezpečnosť produktov priniesť úspornosť výrobcom v rozsahu 290 miliárd EUR ročne v porovnaní so scenárom pokračujúcej fragmentácie. Táto úspornosť vychádza z odstránenia duplicitných certifikácií, zjednodušenej dokumentácie a znížených nákladov na monitoring rôznych národných požiadaviek.

V oblasti cezhraničného elektronického obchodu odhaduje Európska komisia, že odstránenie regulačných bariér môže viesť k nárastu cezhraničného digitálneho obchodu o 2 % a generovať spotrebiteľský prebytok vo výške 13 miliárd EUR ročne. Tieto čísla ilustrujú významný ekonomický potenciál, ktorý harmonizácia uvoľňuje pre podniky všetkých veľkostí.

Globálny trh cezhraničného elektronického obchodu dosahuje podľa analytickej spoločnosti Precedence Research hodnotu 370 miliárd USD v roku 2024 s očakávaným rastom na 1,6 bilióna USD do roku 2033, čo predstavuje zloženú ročnú mieru rastu (CAGR) 18%. Európske MSP, ktoré dokážu efektívne využiť harmonizovaný regulačný rámec, majú príležitosť participovať na tomto dynamicky rastúcom trhu.

4.2.2 Nové trhové príležitosti vznikajúce z regulácií

Regulácie AI Act, CRA a NIS2 generujú významný dopyt po nových produktoch a službách, čo vytvára trhové príležitosti pre MSP s relevantnou expertízou. Tieto príležitosti možno kategorizovať do niekoľkých hlavných segmentov: konzultačné a poradenské služby, technologické riešenia, vzdelávacie služby a certifikačné služby.

Trh konzultačných a poradenských služieb

Komplexnosť nových regulácií vytvára substanciálny dopyt po špecializovanom poradenstve. Podniky, ktoré musia implementovať požiadavky AI Act, CRA alebo NIS2, často nemajú interné kapacity na interpretáciu regulácií, navrhovanie compliance stratégií a implementáciu potrebných opatrení. Tento dopyt otvára priestor pre konzultačné spoločnosti všetkých veľkostí.

Pre MSP v oblasti IT consultingu a právneho poradenstva predstavuje toto príležitosť na rozšírenie portfólia služieb. Špecializácia na konkrétnu reguláciu (napríklad AI Act pre právne kancelárie, CRA pre IT bezpečnostné firmy) môže MSP odlíšiť od generálnych konzultačných spoločností a vytvoriť nišovú expertízu[25] s vysokou pridanou hodnotou.

Podľa prieskumu ISACA z roku 2024 až 67% organizácií plánuje zvýšiť investície do externého poradenstva v oblasti kybernetickej bezpečnosti a compliance v nasledujúcich dvoch rokoch. Tento trend naznačuje rastúci trh, na ktorom môžu MSP s relevantnou expertízou uspieť.

[25] Ide o úzko špecializovanú odbornú expertízu v konkrétnej, pomerne úzkej oblasti

Trh technologických riešení

Regulácie vytvárajú dopyt po technologických nástrojoch, ktoré pomáhajú podnikom dosiahnuť a udržať súlad. Tieto nástroje zahŕňajú niekoľko kategórií.

Nástroje pre riadenie rizík AI systémov umožňujú organizáciám systematicky identifikovať, hodnotiť a riadiť riziká spojené s využívaním AI. Podľa AI Act musia poskytovatelia a nasadzujúce subjekty vysokorizikových AI systémov implementovať systémy riadenia rizík (článok 9). Nástroje automatizujúce časť tohto procesu majú potenciál významnej pridanej hodnoty. Trh AI governance softvérov dosahuje podľa Grand View Research hodnotu 180 miliónov USD v roku 2024 s očakávaným CAGR 35 % do roku 2030.

Platformy pre správu zraniteľností a SBOM reagujú na požiadavky CRA na systematické riadenie zraniteľností produktov s digitálnymi prvkami. SBOM sa stáva štandardom pre dokumentáciu komponentov softvérových produktov a riadenie rizík dodávateľského reťazca. Nástroje na automatizovanú tvorbu a správu SBOM, integrované do vývojárskych procesov, majú rastúci dopyt. Podľa prieskumu Gartner 60 % organizácií plánuje do roku 2025 vyžadovať SBOM od svojich dodávateľov softvéru[26].

Systémy SIEM a monitoring bezpečnosti sú kľúčové pre plnenie požiadaviek NIS2 na detekciu a reakciu na bezpečnostné incidenty. Malé a stredné podniky, ktoré sa stávajú regulovanými subjektmi podľa NIS2, potrebujú riešenia prispôsobené ich veľkosti a rozpočtu. MSP ponúkajúce SIEM-as-a-Service alebo managed security services majú príležitosť osloviť tento segment.

Nástroje pre dokumentáciu a audit trail pomáhajú podnikom vytvárať a udržiavať technickú dokumentáciu požadovanú reguláciami. AI Act požaduje rozsiahlu dokumentáciu pre vysokorizikové systémy (článok 11), CRA vyžaduje technickú dokumentáciu preukazujúcu súlad (článok 31). Automatizované nástroje pre správu dokumentácie a audit trail znižujú administratívnu záťaž a riziko nesúladu.

Tab. č. 8: **Trhové príležitosti v oblasti technologických riešení**

Segment	Regulačný driver	Veľkosť trhu (2024)	Očakávaný rast
AI governance softvér	AI Act - riadenie rizík	180 mil. USD	CAGR 35 %
SBOM nástroje	CRA - supply chain	120 mil. USD	CAGR 28 %
SMB SIEM riešenia	NIS2 - monitoring	2,1 mld. USD	CAGR 12 %
Compliance automation	Všetky regulácie	890 mil. USD	CAGR 18 %
Privacy tech (GDPR+AI)	AI Act + GDPR	3,2 mld. USD	CAGR 22 %

Zdroj: Grand View Research, Gartner, Markets and Markets, 2024

[26] **Gartner.** *Predicts 2023: Cybersecurity – SBOMs Become Foundational to Software Supply Chain Security.* Stamford, CT: Gartner, 2023

Trh vzdelávacích služieb

Regulácie vytvárajú potrebu systematického vzdelávania zamestnancov. AI Act v článku 4 zavádza požiadavku AI gramotnosti, podľa ktorej poskytovatelia a nasadzujúce subjekty musia zabezpečiť, aby ich zamestnanci mali dostatočnú úroveň AI gramotnosti. NIS2 vyžaduje pravidelné školenia v oblasti kybernetickej bezpečnosti pre zamestnancov regulovaných subjektov.

Pre vzdelávacie inštitúcie a špecializované školiace spoločnosti to predstavuje príležitosť na vývoj nových kurzov a certifikačných programov. MSP v oblasti e-learningu a školeniam majú príležitosť vytvoriť škálovateľné digitálne vzdelávacie produkty pokrývajúce požiadavky regulácií.

Podľa LinkedIn Learning Reportu 2024 patria kybernetická bezpečnosť a AI medzi top 5 najžiadanejších oblastí pre firemné vzdelávanie globálne. Dopyt po špecializovaných kurzoch zameraných na regulačné požiadavky (AI Act compliance, NIS2 awareness) je zatiaľ nedostatočne pokrytý, čo predstavuje trhovú niku pre agilné MSP.[27]

Trh certifikačných a auditných služieb

AI Act a CRA vytvárajú dopyt po nezávislom posudzovaní zhody. Pre určité kategórie vysokorizikových AI systémov je požadované posúdenie notifikovaným orgánom (tretia strana). CRA vyžaduje pre produkty s digitálnymi prvkami kritickej triedy posúdenie zhody treťou stranou.

Pre MSP s expertízou v oblasti auditovania a certifikácie existuje príležitosť stať sa notifikovaným orgánom alebo poskytovať podporné služby pre proces certifikácie. Hoci samotná notifikácia vyžaduje splnenie náročných kritérií (akreditácia podľa normy ISO/IEC 17065), MSP majú príležitosť pôsobiť ako subdodávatelia notifikovaných orgánov alebo poskytovať pre-certifikačné audity a gap analýzy.

Podľa správy A-LIGN 2025 Compliance Benchmark Report až 92 % organizácií podstupuje dva alebo viac bezpečnostných auditov ročne, pričom 61 % uvádza, že regulované subjekty od nich vyžadujú dokladovanie bezpečnostnej certifikácie ako podmienku spolupráce. Tento trend ilustruje rastúci význam certifikácií a auditov v obchodných vzťahoch.

4.2.3 Bruselský efekt a globálna konkurencieschopnosť

Fenomén označovaný ako Bruselský efekt, teoreticky rozpracovaný profesorkou Anu Bradford z Columbia Law School, popisuje schopnosť Európskej únie exportovať svoje regulačné štandardy za hranice svojej jurisdikcie prostredníctvom trhových mechanizmov. Pre MSP pôsobiace v regulovaných oblastiach má tento fenomén významné strategické implikácie.[28]

[27] **LinkedIn Learning.** *Workplace Learning Report 2024.* Sunnyvale, CA: LinkedIn Corporation, 2024.
[28] BRADFORD, Anu. **The Brussels Effect.** *Northwestern University Law Review*, 2012, roč. 107, č. 1, s. 1–67.

Mechanizmus Bruselského efektu

Bruselský efekt funguje prostredníctvom dvoch hlavných kanálov. Prvý kanál je de facto efekt, keď sa nadnárodné spoločnosti dobrovoľne rozhodnú aplikovať prísnejšie európske štandardy globálne, pretože je to pre ne efektívnejšie než udržiavať rozdielne štandardy pre rôzne trhy. Druhý kanál je de iure efekt, keď tretie krajiny prijímajú legislatívu inšpirovanú alebo priamo kopírujúcu európske regulácie, či už z dôvodu uľahčenia obchodu s EÚ alebo ako vzor pre vlastnú reguláciu.

V kontexte AI regulácie pozorujeme oba tieto kanály v akcii. Veľké technologické spoločnosti ako Microsoft, Google a IBM oznámili zámery aplikovať princípy AI Act globálne alebo vo významnej časti svojich operácií. Súčasne krajiny ako Brazília, Kanada, Japonsko a India vyvíjajú alebo už prijali AI legislatívu, ktorá vykazuje významné podobnosti s európskym prístupom.

Implikácie pre MSP

Pre slovenské MSP má Bruselský efekt niekoľko významných implikácií. Predovšetkým, investície do súladu s EÚ reguláciami nie sú len nákladom pre prístup na európsky trh, ale môžu byť aj investíciou do globálnej konkurencieschopnosti. MSP, ktoré dosiahnu súlad s AI Act alebo CRA, budú mať výhodnejšiu štartovaciu pozíciu na tretích trhoch, ktoré prijmú podobné regulácie.

Slovenské MSP poskytujúce technologické riešenia alebo služby môžu ťažiť z toho, že ich produkty navrhnuté pre súlad s EÚ reguláciami budú relevantné aj na tretích trhoch. Napríklad MSP vyvíjajúce nástroj pre riadenie rizík AI systémov podľa požiadaviek AI Act môže tento nástroj potenciálne predávať aj na trhoch v Kanade, Brazílii alebo Indii, kde sa očakáva prijatie podobnej regulácie.

Konkurenčná výhoda - early adopters

MSP, ktoré sa včas pripravia na regulačné požiadavky, môžu získať konkurenčnú výhodu oproti konkurentom z tretích krajín, ktorí budú musieť regulačné požiadavky plniť až pri vstupe na európsky trh. Táto výhoda je obzvlášť relevantná v odvetviach, kde európsky trh predstavuje významnú časť globálneho dopytu.

Podľa údajov UNCTAD predstavuje Európska únia druhý najväčší trh pre digitálne služby globálne, s hodnotou 260 miliárd USD v roku 2023. Pre poskytovateľov digitálnych produktov a služieb je prístup na tento trh strategickou prioritou a súlad s EÚ reguláciami je nevyhnutnou podmienkou.

Tab. č. 9: **Prehľad krajín s AI legislatívou inšpirovanou EÚ prístupom**

Krajina/región	Status legislatívy	Podobnosti s AI Act
Brazília	Návrh zákona v parlamente (2024)	Rizikový prístup, požiadavky na transparentnosť
Kanada	AIDA - návrh zákona (2023)	Kategorizácia podľa rizika, požiadavky na dokumentáciu
Japonsko	AI Guidelines (2024, soft law)	Dôraz na transparentnosť a bezpečnosť
India	Príprava návrhu (2024)	Rizikový prístup v diskusii
Južná Kórea	AI Act prijatý (2025)	Veľmi podobná štruktúra ako EÚ AI Act
Singapur	AI Governance Framework (2024)	Princípy zodpovednej AI, dobrovoľné štandardy

Zdroj: OECD AI Policy Observatory, narodne legislativne zdroje, 2024-2025

4.2.4 Prístup na regulovane trhy a verejné zákazky

Regulácie NIS2 a AI Act vytvárajú kategórie regulovaných subjektov, ktoré musia plniť určité požiadavky, a ktoré súčasne vyžadujú plnenie týchto požiadaviek od svojich dodávateľov. Pre MSP pôsobiace v dodávateľských reťazcoch týchto subjektov to znamená nové požiadavky, ale aj príležitosti. Súlad s požiadavkami na kybernetickú bezpečnosť, riadenie rizík a zodpovedné využívanie technológií sa postupne stáva faktickou podmienkou prístupu k regulovaným trhom, k zákazkám od veľkých podnikov a čoraz častejšie aj k verejnému obstarávaniu.

Dodávateľský reťazec regulovaných subjektov

NIS2 kategorizuje subjekty na základné a dôležité podľa ich veľkosti a sektora pôsobnosti. Tieto subjekty musia implementovať opatrenia na riadenie rizík kybernetickej bezpečnosti vrátane bezpečnosti dodávateľského reťazca (článok 21 ods. 2 písmeno d). V praxi to znamená, že regulované subjekty budú od svojich dodávateľov vyžadovať dokladovanie prístupu ku kybernetickej bezpečnosti.

Podľa prieskumu A-LIGN 2025 až 61 %regulovaných subjektov už teraz vyžaduje od dodávateľov bezpečnostnú certifikáciu ako podmienku spolupráce. S nadobudnutím účinnosti NIS2 v októbri 2024 a prebiehajúcou implementáciou v členských štátoch sa očakáva, že tento podiel ešte vzrastie.

Pre MSP pôsobiace ako dodávatelia pre veľké podniky alebo verejný sektor to znamená, že investície do kybernetickej bezpečnosti a získanie relevantných certifikácií (napríklad ISO 27001) sa stávajú nevyhnutnosťou pre udržanie existujúcich a získanie nových kontraktov. MSP, ktoré budú schopné preukázať robustný prístup ku kybernetickej bezpečnosti, získajú konkurenčnú výhodu oproti dodávateľom bez takéhoto preukazu.

V kontexte uvedeného možno zároveň poukázať na **asymetrický vzťah medzi veľkými regulovanými podnikmi a MSP v dodávateľských reťazcoch**. Technologické regulácie umožňujú prenášať regulačné a bezpečnostné požiadavky aj na menších dodávateľov, ktorí sami často nepodliehajú priamej regulácii alebo by im právne predpisy takéto povinnosti v obdobnom rozsahu samostatne neukladali. Veľké podniky, ktoré čelia zákonným povinnostiam a vysokým sankčným rizikám, majú prirodzenú motiváciu externalizovať časť regulačného a bezpečnostného bremena smerom nadol v dodávateľskom reťazci

prostredníctvom zmluvných požiadaviek, auditných práv, povinných certifikácií či oznamovacích povinností pri incidentoch.

Pre MSP je problémom najmä to, že vzhľadom na svoju obmedzenú vyjednávaciu silu spravidla nemajú reálnu možnosť tieto dodatočné náklady preniesť ďalej, či už na svojich odberateľov, alebo na ďalšie články reťazca. Náklady na certifikácie, interné procesy, dokumentáciu, školenia či technické opatrenia preto často znášajú samy, a to bez primeranej kompenzácie v cene. Výsledkom môže byť znižovanie marží, oslabovanie investičnej kapacity a v konečnom dôsledku aj zhoršenie konkurencieschopnosti MSP, najmä v prípadoch, keď pôsobia ako subdodávatelia vo vysoko regulovaných sektoroch. Regulácie tak v praxi nepriamo posilňujú trhovú pozíciu väčších podnikov, ktoré lepšie absorbujú zvýšené náklady na regulačné požiadavky.

Zároveň však platí, že MSP, ktoré budú schopné tieto požiadavky splniť a následne preukázať svoju bezpečnostnú a organizačnú pripravenosť, môžu získať významnú konkurenčnú výhodu. Najmä v európskom prostredí neustále sa zvyšujúcej regulácie sa dôveryhodný dodávateľ stáva pre veľké podniky prijateľnejšou alternatívou oproti dodávateľovi, ktorý síce môže ponúkať nižšiu cenu, ale predstavuje zvýšené regulačné alebo bezpečnostné riziko.

Verejné zákazky a bezpečnostné požiadavky

Verejný sektor predstavuje významný trh pre MSP, pričom EÚ aktívne podporuje účasť MSP vo verejných zákazkách. Súčasne verejné inštitúcie čelia rastúcim požiadavkám na kybernetickú bezpečnosť a zodpovedné využívanie AI, čo sa prenáša do požiadaviek na dodávateľov.

Smernica o verejnom obstarávaní (2014/24/EÚ) umožňuje verejným obstarávateľom zahrnúť technické špecifikácie a kritériá na vyhodnotenie ponúk, zahrnujúce bezpečnostné požiadavky. S implementáciou NIS2 a AI Act možno očakávať rastúci podiel zákaziek, ktoré budú obsahovať explicitné požiadavky na súlad s týmito reguláciami alebo ekvivalentné bezpečnostné štandardy.

Pre MSP usilujúce o účasť vo verejných zákazkách sa stáva strategickou nevyhnutnosťou pripraviť sa na tieto požiadavky. Zavedenie systému riadenia informačnej bezpečnosti, získanie certifikácie ISO 27001 alebo ekvivalentnej a schopnosť preukázať zodpovedný prístup k AI môžu významne zvýšiť šancu na úspech v súťažiach.

Sektorové príležitosti

Niektoré sektory ponúkajú obzvlášť významné príležitosti pre MSP v kontexte nových regulácií.

Zdravotníctvo je sektorom, kde AI Act kategorizuje viaceré aplikácie ako vysokorizikové (príloha III, bod 5) a kde NIS2 zahŕňa poskytovateľov zdravotnej starostlivosti medzi dôležité subjekty. Dopyt po bezpečných a súladných AI riešeniach pre zdravotníctvo je vysoký a MSP so špecializáciou v health tech majú príležitosť.

Finančné služby sú sektorom s tradične prísnou reguláciou, kde subjekty majú skúsenosti s compliance a aktívne hľadajú inovatívne riešenia. Smernica DORA (Digital Operational Resilience Act) dopĺňa NIS2 špecifickými požiadavkami pre finančný sektor, čo generuje dopyt po špecializovaných riešeniach.

Energetika a kritická infraštruktúra sú sektormi, kde NIS2 kategorizuje väčšinu subjektov ako základné s najvyššími požiadavkami. Modernizácia energetickej infraštruktúry a rozvoj smart grids vytvárajú dopyt po bezpečných IoT riešeniach v súlade s CRA.

Verejná správa prechádza digitálnou transformáciou, pričom musí súčasne plniť požiadavky na bezpečnosť (NIS2 sa vzťahuje na subjekty verejnej správy) a zodpovedné využívanie AI. MSP ponúkajúce riešenia pre e-government majú príležitosť.

4.2.5 Bariéry a výzvy pri využívaní trhových príležitosti

Napriek významným príležitostiam, ktoré nové regulácie vytvárajú, MSP čelia pri ich využívaní radu bariér a výziev. Pochopenie týchto prekážok je kľúčové pre realistické hodnotenie potenciálu a formuláciu stratégií na ich prekonanie.

Pretrvávajúca implementačná fragmentácia

Hoci AI Act a CRA sú nariadenia priamo aplikovateľné vo všetkých členských štátoch a NIS2 je smernica s cieľom harmonizácie, v praxi pretrváva určitá miera fragmentácie v implementácii a výkone. Členské štáty majú mieru voľnej úvahy v niektorých aspektoch, čo môže viesť k rozdielom v praktickom uplatňovaní.

Napríklad NIS2 umožňuje členským štátom rozšíriť pôsobnosť na ďalšie sektory alebo menšie subjekty nad rámec minimálnych požiadaviek smernice. Niektoré členské štáty môžu pristupovať k výkonu a sankciám rôznym spôsobom. Pre MSP pôsobiace na viacerých národných trhoch to znamená, že aj napriek harmonizácii je potrebné sledovať špecifiká implementácie v jednotlivých krajinách.

Nedostatok kvalifikovanej pracovnej sily

Globálny nedostatok odborníkov v oblasti kybernetickej bezpečnosti a AI predstavuje významnú bariéru pre MSP. Podľa štúdií (ISC)2 chýba globálne 3,4 milióna profesionálov v oblasti kybernetickej bezpečnosti, pričom v Európe je tento deficit odhadovaný na 350 000 pozícií. V oblasti AI a machine learning je situácia podobná, pričom dopyt po odborníkoch prevyšuje ponuku.[29]

Pre MSP je obťažné konkurovať veľkým korporáciám v nábore obmedzeného počtu talentov. Veľké spoločnosti môžu ponúknuť vyššie mzdy, komplexnejšie benefity a prestížnejšie projekty. MSP musia hľadať alternatívne stratégie, ako je investícia do interného

[29] **(ISC)².** *Cybersecurity Workforce Study 2023.* Alexandria, VA: (ISC)², 2023.

rozvoja zamestnancov, spolupráca s univerzitami, využívanie freelancerov a konzultantov alebo partnerstvá s inými MSP pre zdieľanie expertízy.

Tab. č. 10: **Globálny deficit odborníkov v kľúčových oblastiach**

Oblasť	Globálny deficit	Deficit v Európe
Kybernetická bezpečnosť	3,4 milióna	cca 350 000
AI a Machine Learning	cca 1 milión	cca 150 000
Data Science	cca 700 000	cca 100 000
Cloud Security	cca 500 000	cca 80 000

Zdroj: (ISC)2 Cybersecurity Workforce Study 2024, LinkedIn Talent Insights, World Economic Forum

Finančné bariéry a prístup ku kapitálu

Využitie regulačných príležitostí často vyžaduje počiatočné investície do rozvoja produktov, získania certifikácií a budovania obchodných kapacít. Pre MSP môže byť prístup ku kapitálu potrebnému na tieto investície obmedzený.

Podľa ECB Survey on the Access to Finance of Enterprises (SAFE) z roku 2024 až 8 % MSP v eurozóne uvádza prístup k financovaniu ako najvýznamnejší problém, pričom v niektorých členských štátoch (vrátane Slovenska) je tento podiel vyšší. Inovatívne MSP v technologických sektoroch často narážajú na nepochopenie ich obchodného modelu zo strany tradičných poskytovateľov financovania.[30]

Riešením môžu byť alternatívne zdroje financovania ako rizikový kapitál, granty z programov EÚ (Horizont Europe, Digital Europe, Nástroj na prepájanie Európy), národné schémy podpory inovácií alebo crowdfunding. MSP by mali aktívne vyhľadávať a využívať tieto možnosti na financovanie investícií do compliance a rozvoja produktov pre regulované trhy.

Jazykové a kultúrne bariéry

Napriek jednotnému trhu EÚ existujú pretrvávajúce jazykové a kultúrne bariéry, ktoré môžu komplikovať cezhraničné podnikanie MSP. Regulačná dokumentácia, normy a usmernenia sú často dostupné primárne v angličtine alebo v jazykoch veľkých členských štátov, čo zvyšuje náklady pre MSP z menších krajín.

Kultúrne rozdiely v obchodnej praxi, preferenciách zákazníkov a vzťahoch s autoritami môžu tiež ovplyvňovať úspešnosť MSP na zahraničných trhoch. MSP vstupujúce na nové trhy musia investovať do pochopenia lokálnych špecifík a budovania vzťahov s lokálnymi partnermi.

[30] **European Central Bank (ECB).** *Survey on the Access to Finance of Enterprises (SAFE) – April to September 2024*

Konkurencia zo strany veľkých hráčov

Trhové príležitosti vytvorené reguláciami priťahujú aj veľké korporácie a medzinárodné konzultačné spoločnosti. Tieto subjekty majú významné zdroje na rýchly vývoj produktov, marketing a budovanie značky, čo môže vytláčať MSP z lukratívnych segmentov trhu.

MSP môžu uspieť prostredníctvom špecializácie na špecifické segmenty, kde ich expertíza prevyšuje generálnych hráčov, prostredníctvom flexibility a schopnosti rýchlo reagovať na špecifické potreby zákazníkov, prostredníctvom budovania dlhodobých vzťahov so zákazníkmi založených na dôvere a personalizovanom prístupe a prostredníctvom spolupráce s inými MSP pre budovanie komplexnejších riešení.

4.2.6 Zhrnutie a strategické odporúčania

Regulácie AI Act, CRA a NIS2 vytvárajú pre MSP komplexnú krajinu trhových príležitostí a výziev. Úspešné využitie týchto príležitostí vyžaduje strategický prístup, ktorý kombinuje realistické hodnotenie vlastných kapacít s proaktívnym vyhľadávaním a využívaním dostupných podporných nástrojov.

Kľúčové zistenia

Harmonizácia regulačného rámca naprieč EÚ znižuje transakčné náklady cezhraničného podnikania a vytvára jednotný trh so 450 miliónmi spotrebiteľov pre súladné produkty a služby. MSP, ktoré dosiahnu súlad s EÚ reguláciami, získavajú prístup na celý tento trh s jedným setom požiadaviek.

Regulácie generujú významný dopyt po nových produktoch a službách v oblasti compliance, kybernetickej bezpečnosti a dôveryhodnej AI. Trhy v týchto oblastiach rastú dvojciferným tempom a ponúkajú príležitosti pre MSP s relevantnou expertízou.

Bruselský efekt rozširuje relevanciu EÚ regulácií za hranice Európy. MSP investujúce do súladu s EÚ štandardmi budujú kapacity relevantné aj pre tretie trhy prijímajúce podobné regulácie.

Pretrvávajú bariéry vrátane implementačnej fragmentácie, nedostatku kvalifikovanej pracovnej sily, finančných obmedzení a konkurencie zo strany veľkých hráčov. Prekonanie týchto bariér vyžaduje cielené stratégie a využitie dostupnej podpory.

Strategické odporúčania pre MSP

Prvým odporúčaním je identifikácia a zameranie sa na konkrétny trhový segment. MSP by mali analyzovať svoje existujúce kompetencie a identifikovať segmenty, kde môžu priniesť najvyššiu pridanú hodnotu. Špecializácia na konkrétnu reguláciu, sektor alebo typ služby umožňuje budovať hlbokú expertízu a odlíšiť sa od konkurencie.

Druhým odporúčaním je využitie CE označenia a harmonizovaných noriem ako konkurenčnej výhody. Investície do posúdenia zhody a získania CE označenia by MSP mali komunikovať ako indikátor kvality a dôveryhodnosti smerom k zákazníkom. Súlad s harmonizovanými normami zjednodušuje dokladovanie zhody a buduje dôveru.

Tretím odporúčaním je budovanie partnerstiev pre rozšírenie kapacít. MSP môžu prekonať obmedzenia vlastných zdrojov prostredníctvom strategických partnerstiev s inými MSP, univerzitami, výskumnými inštitúciami a väčšími spoločnosťami. Partnerstvá umožňujú zdieľanie nákladov, dopĺňanie kompetencií a prístup k väčším projektom.

Štvrtým odporúčaním je proaktívne vyhľadávanie financovania. MSP by mali aktívne monitorovať a využívať dostupné grantové schémy (Horizont Europe, Digital Europe, národné programy), ale aj alternatívne zdroje financovania ako rizikový kapitál a strategickí investori.

Piatym odporúčaním je investícia do ľudského kapitálu. Dlhodobá konkurencieschopnosť MSP závisí od kompetencií ich zamestnancov. Investície do školení, certifikácií a vytvárania atraktívneho pracovného prostredia sú kľúčové pre pritiahnuť a udržať talenty v konkurenčnom prostredí.

Pre slovenské MSP bude kľúčové prepojiť sa na európske siete a iniciatívy, využívať služby EDIH a aktívne sledovať vývoj na jednotlivých trhoch. Podniky, ktoré dokážu trhové príležitosti včas identifikovať a strategicky využiť, majú potenciál transformovať regulačnú zmenu na motor rastu a medzinárodnej expanzie.

4.3 Reputačné efekty a dôvera zákazníkov

V digitalizovanej ekonomike sa dôvera zákazníkov stáva jedným z najcennejších nehmotných aktív podniku. Kybernetické bezpečnostné incidenty, zneužitie osobných údajov alebo neetické využívanie umelej inteligencie môžu spôsobiť významné reputačné škody s dlhodobými dôsledkami na obchodné výsledky. Regulácie AI Act, CRA a NIS2 vytvárajú rámec, v ktorom podniky môžu budovať a preukázať svoju dôveryhodnosť systematickým prístupom k bezpečnosti, transparentnosti a etike.

Pre malé a stredné podniky predstavuje budovanie dôvery špecifickú výzvu aj príležitosť. Na jednej strane MSP nemajú veľkú vedomosť verejnosti, ako veľké korporácie a musia si dôveru zákazníkov budovať od základov. Na druhej strane práve demonštrácia nadštandardného prístupu k bezpečnosti a etike môže MSP odlíšiť od konkurencie a vytvoriť trvalú konkurenčnú výhodu.

Táto podkapitola analyzuje empirické dôkazy o vplyve kybernetickej bezpečnosti a etických praktík na obchodné výsledky, skúma mechanizmy, ktorými regulácie umožňujú budovanie dôvery, a poskytuje praktické odporúčania pre MSP na transformáciu compliance povinností na reputačnú výhodu.

4.3.1 Kybernetická bezpečnosť ako konkurenčný diferenciátor

Kybernetická bezpečnosť sa v posledných rokoch transformovala z čisto technickej a operačnej záležitosti na strategický faktor ovplyvňujúci obchodné vzťahy, prístup k zákazkám a celkovú reputáciu podniku. Empirické štúdie dokumentujú rastúci význam bezpečnostných certifikácií a preukázaných bezpečnostných praktík v rozhodovaní zákazníkov a obchodných partnerov.

Empirické dôkazy o obchodnom význame bezpečnosti

Podľa výskumu A-LIGN publikovaného v roku 2024 až 72 % organizácií podstúpilo bezpečnostný audit alebo hodnotenie s cieľom získať novú zákazku alebo uzavrieť obchodnú dohodu. Toto číslo ilustruje, že bezpečnostné hodnotenia sa stali štandardnou súčasťou obchodného procesu v mnohých sektoroch, nie výnimočnou požiadavkou.

Ešte výpovednejším je zistenie, že 29 % organizácií v tom istom výskume uviedlo, že stratili potenciálny kontrakt práve preto, že nedokázali predložiť požadovanú bezpečnostnú certifikáciu alebo uspokojivo odpovedať na bezpečnostný dotazník. Pre MSP usilujúce o zákazky od väčších korporácií alebo vo verejnom sektore je toto riziko obzvlášť relevantné.

Prieskum PwC Global Digital Trust Insights z roku 2024 potvrdzuje strategický význam kybernetickej bezpečnosti. Podľa tohto prieskumu 55 % manažérov v retailovom sektore identifikovalo zvýšenú dôveru zákazníkov ako kľúčový prínos investícií do kybernetickej bezpečnosti. Ďalších 44 % manažérov uviedlo, že kybernetická bezpečnosť funguje ako katalyzátor integrity značky a celkovej reputácie spoločnosti.[31]

Tab. č. 11: **Obchodný význam kybernetickej bezpečnosti – kľúčové štatistiky**

Indikátor	Hodnota	Zdroj
Organizácie, ktoré podstúpili audit pre získanie zákazky	72 %	A-LIGN 2024
Organizácie, ktoré stratili kontrakt kvôli chýbajúcej certifikácii	29 %	A-LIGN 2024
Manažéri vnímajúci bezpečnosť ako zdroj dôvery zákazníkov	55 %	PwC 2024
Manažéri vnímajúci bezpečnosť ako katalyzátor integrity značky	44 %	PwC 2024
Organizácie vykonávajúce 2+ bezpečnostné audity ročne	92 %	A-LIGN 2025
Regulované subjekty vyžadujúce certifikát od dodávateľov	61 %	A-LIGN 2025

Zdroj: A-LIGN Research 2024, A-LIGN 2025 Compliance Benchmark Report, PwC Global Digital Trust Insights 2024

Náklady bezpečnostných incidentov

Reputačný význam kybernetickej bezpečnosti je ešte zreteľnejší pri pohľade na náklady bezpečnostných incidentov. Podľa IBM Cost of a Data Breach Report 2024 dosahujú priemerné náklady na jeden bezpečnostný incident globálny priemer 4,88 milióna USD, čo predstavuje 10% medziročný nárast. Tieto náklady zahŕňajú priame náklady na reakciu a nápravu, právne náklady a pokuty, ako aj nepriame náklady v podobe straty zákazníkov a reputačného poškodenia.[32]

Pre menšie podniky sú relatívne dopady ešte výraznejšie. Podľa tej istej štúdie podniky s menej ako 500 zamestnancami čelia priemerným nákladom 3,31 milióna USD na incident.

[31] **A-LIGN.** *2024 Compliance Benchmark Report.* Tampa, FL: A-LIGN, 2024 **PwC.** *Global Digital Trust Insights 2024.* London: PricewaterhouseCoopers, 2024

[32] **IBM Security.** *Cost of a Data Breach Report 2024.* Armonk, NY: IBM Corporation, 2024.

Hoci je absolútna suma nižšia ako u veľkých podnikov, pre MSP môže takáto suma predstavovať existenčné ohrozenie.

Štatistiky spoločnosti Verizon v Data Breach Investigations Report ukazujú, že až 60 % malých podnikov, ktoré zažijú významný kybernetický útok, ukončí svoju činnosť do šiestich mesiacov od incidentu. Toto dramatické číslo ilustruje, že pre MSP nie je kybernetická bezpečnosť len otázkou compliance, ale existenčnou prioritou.[33]

Transformácia compliance na konkurenčnú výhodu

V kontexte týchto dát sa investície do kybernetickej bezpečnosti a získavania certifikácií javia nielen ako náklad, ale ako strategická investícia s merateľnou návratnosťou. MSP, ktoré dokážu demonštrovať robustný prístup k bezpečnosti, majú výhodu pri získavaní zákaziek, udržaní existujúcich zákazníkov a budovaní dlhodobej reputácie.

Certifikácia ISO 27001 (systém riadenia informačnej bezpečnosti) sa stáva de facto štandardom, ktorý očakávajú zákazníci v mnohých sektoroch. Podľa údajov ISO Survey 2023 počet certifikovaných organizácií rastie medziročne o približne 20 %, čo naznačuje rastúce očakávania trhu. Pre MSP môže získanie tejto certifikácie predstavovať významnú investíciu, ale súčasne vytvoriť jasný diferenciátor voči necertifikovanej konkurencii.

Okrem formálnych certifikácií môžu MSP demonštrovať svoj prístup k bezpečnosti aj inými spôsobmi, ako sú transparentná komunikácia o bezpečnostných praktikách, publikovanie bezpečnostných politík a postupov, účasť v programoch zodpovedného zverejňovania zraniteľností (responsible disclosure) alebo referencie od existujúcich zákazníkov potvrdzujúce bezpečnostné štandardy.[34]

4.3.2 Eticky prístup k AI ako hodnotová propozícia

S rastúcim nasadzovaním systémov umelej inteligencie narastajú aj obavy verejnosti ohľadom ich potenciálneho zneužitia. AI Act reaguje na tieto obavy zavedením rámca, ktorý zakazuje určité praktiky a reguluje vysokorizikové aplikácie. Pre MSP vyvíjajúce alebo nasadzujúce AI systémy vytvára tento rámec príležitosť odlíšiť sa prostredníctvom demonštrácie etického prístupu.

Zakázané praktiky a ich reputačné implikácie

AI Act v článku 5 definuje zoznam zakázaných praktík AI, ktoré sú považované za neprijateľné z hľadiska základných práv a európskych hodnôt. Pochopenie týchto zákazov je dôležité nielen pre zabezpečenie súladu, ale aj pre pochopenie spoločenských očakávaní ohľadom zodpovedného využívania AI.

[33] **Verizon.** *2024 Data Breach Investigations Report (DBIR).* New York: Verizon Enterprise, 2024
[34] **International Organization for Standardization (ISO).** *The ISO Survey of Management System Standard Certifications 2023.* Geneva: ISO, 2023

- Podprahové a manipulatívne techniky sú zakázané, ak sú využívané na ovplyvnenie správania osôb spôsobom, ktorý môže spôsobiť fyzickú alebo psychologickú ujmu. Tento zákaz reflektuje obavy z využívania AI na nevedomú manipuláciu spotrebiteľov a občanov. Pre MSP to znamená, že akékoľvek AI riešenia pre marketing, predaj alebo ovplyvnenie rozhodovania musia byť navrhnuté s rešpektom k autonómii a informovanému rozhodovaniu používateľov.

- Využívanie zraniteľnosti špecifických skupín (na základe veku, zdravotného postihnutia alebo socioekonomickej situácie) na ovplyvnenie ich správania je zakázané. Tento zákaz má obzvlášť význam pre MSP pôsobiace v oblastiach ako finančné služby, zdravotníctvo alebo vzdelávanie, kde môžu AI systémy interagovať so zraniteľnými skupinami.

- Sociálne skórovanie verejnými orgánmi alebo v ich mene je zakázané, ak vedie k nepriaznivému alebo neopodstatnenému zaobchádzaniu s jednotlivcami. Pre MSP vyvíjajúce riešenia pre verejný sektor je dôležité zabezpečiť, že ich systémy neumožňujú takéto využitie.

- Rozpoznávanie emócií na pracovisku a vo vzdelávacích inštitúciách je zakázané s výnimkami pre medicínske alebo bezpečnostné účely. MSP vyvíjajúce riešenia pre HR alebo vzdelávanie musia toto obmedzenie zohľadniť pri návrhu svojich produktov.

- Biometrická kategorizácia na základe citlivých atribútov (rasa, politické názory, náboženstvo, sexuálna orientácia) je zakázaná. Pre MSP pracujúce s biometrickými dátami je nevyhnutné zabezpečiť, že ich systémy nevykonávajú takúto kategorizáciu ani implicitne.

Tab. č. 12: **Prehľad zakázaných AI praktík podľa článku 5 AI Act**

Zakázaná praktika	Popis	Relevancia pre MSP
Podprahová manipulácia	Techniky mimo vedomia osoby spôsobujúce ujmu	Marketing, predaj
Využívanie zraniteľnosti	Zameranie na vek, postihnutie, socioekonomickú situáciu	Financie, zdravotníctvo
Sociálne skórovanie	Hodnotenie vedúce k nepriaznivému zaobchádzaniu	Verejný sektor, HR
Rozpoznávanie emócií	Na pracovisku a v školách (s výnimkami)	HR tech, EdTech
Biometrická kategorizácia	Na základe citlivých atribútov	Biometrické riešenia
Scraping tváre	Necielený zber obrazov tváre z internetu/CCTV	Bezpečnostné riešenia

Zdroj: Nariadenie (EU) 2024/1689 (AI Act), článok 5

Verejné vnímanie AI a jeho implikácie

Verejné vnímanie umelej inteligencie je charakterizované ambivalenciou, kombináciou nádeje z potenciálnych prínosov a obáv z rizík. Podľa Eurobarometra z roku 2024 až 66 % európskych občanov vyjadruje určitú mieru obáv ohľadom využívania AI v spoločnosti, hoci väčšina súčasne uznáva jej potenciálne prínosy.

Obavy sa sústreďujú na niekoľko hlavných oblastí: strata pracovných miest v dôsledku automatizácie, súkromie a ochrana osobných údajov, transparentnosť rozhodovania algoritmov, potenciál pre diskrimináciu a predsudky v AI systémoch a zníženie ľudskej kontroly nad dôležitými rozhodnutiami. Pre MSP vyvíjajúce AI riešenia je pochopenie týchto obáv kľúčové pre návrh produktov, ktoré budú akceptované koncovými používateľmi.[35]

Spoločnosti, ktoré proaktívne adresujú tieto obavy prostredníctvom transparentnej komunikácie, etických záruk a používateľsky prívetivých kontrolných mechanizmov, môžu budovať konkurenčnú výhodu. Naopak, spoločnosti, ktoré ignorujú verejné obavy alebo sú vnímané ako zneužívajúce AI, čelia riziku reputačného poškodenia a straty dôvery zákazníkov.[36]

Budovanie dôveryhodnosti prostredníctvom transparentnosti

AI Act v článku 13 stanovuje požiadavky na transparentnosť pre vysokorizikové AI systémy. Tieto požiadavky zahŕňajú poskytovanie zrozumiteľných informácií používateľom o funkčnosti systému, jeho obmedzeniach a správnom používaní. Pre MSP môže transparentnosť presahovať minimálne regulačné požiadavky a stať sa kľúčovým prvkom hodnotovej propozície.

Konkrétne prístupy k budovaniu dôveryhodnosti prostredníctvom transparentnosti zahŕňajú zrozumiteľnú dokumentáciu algoritmov a ich rozhodovacej logiky prístupnú v primeranej miere pre rôzne cieľové skupiny, jasnú komunikáciu o tom, na čo je AI systém určený a na čo nie, otvorenú komunikáciu o známych obmedzeniach a potenciálnych rizikách, pravidelné reportovanie o výkonnosti a presnosti systémov a mechanizmy pre spätnú väzbu a sťažnosti od používateľov.

Pre MSP môže takáto úroveň transparentnosti slúžiť ako diferenciátor voči veľkým technologickým spoločnostiam, ktoré sú často vnímané ako netransparentné ohľadom fungovania svojich algoritmov. Lokálne MSP s priamym vzťahom k zákazníkom majú príležitosť budovať dôveru prostredníctvom osobného prístupu a otvorenej komunikácie.

4.3.3 Kvantifikácia nákladov reputačných škôd

Reputačné škody v dôsledku bezpečnostných incidentov alebo neetických praktík majú merateľné finančné dopady. Pochopenie týchto nákladov pomôže MSP zdôvodniť investície do bezpečnosti a etiky ako preventívne opatrenia s pozitívnou návratnosťou.

Priame a nepriame náklady incidentov

Náklady bezpečnostných incidentov možno rozčleniť do niekoľkých kategórií. Priame náklady zahŕňajú náklady na detekciu a eskaláciu incidentu, náklady na forenznú

[35] **European Commission.** *Special Eurobarometer 554 – Artificial Intelligence and the Future of Digital Technologies.* Brussels: European Commission, Directorate-General for Communication, 2024

[36] **uropean Commission.** *Special Eurobarometer 554 – Artificial Intelligence and the Future of Digital Technologies.* Brussels: European Commission, 2024.

analýzu, náklady na notifikáciu dotknutých osôb podľa požiadaviek GDPR, náklady na právne služby a prípadné súdne konania, pokuty od regulačných orgánov a náklady na technickú nápravu a posilnenie bezpečnosti.

Nepriame náklady sú často významnejšie a dlhodobejšie. Zahŕňajú stratu zákazníkov v dôsledku narušenia dôvery, zníženie trhovej hodnoty spoločnosti, zvýšené náklady na získavanie nových zákazníkov, vyššie poistné prémie a sťažený prístup k poisteniu a negatívny dopad na morálku zamestnancov a schopnosť pritiahnuť talenty.

Podľa IBM štúdie predstavujú nepriame náklady súvisiace so stratou zákazníkov až 38 % celkových nákladov bezpečnostného incidentu. Pre MSP, ktoré sú často závislé na menšom počte kľúčových zákazníkov, môže strata dôvery aj jedného významného zákazníka mať ničivý dopad.

Tab. č. 13: **Štruktúra nákladov bezpečnostného incidentu**

Kategória nákladov	Podiel na celkových nákladoch	Príklad pre MSP
Detekcia a eskalácia	11 %	Forenzná analýza, externý audit
Notifikácia	6 %	Komunikácia s dotknutými, regulátorom
Reakcia po incidente	28 %	Právne služby, technická náprava
Strata zákazníkov	38 %	Odchod klientov, nižší predaj
Pokuty a regulačné náklady	12 %	GDPR pokuty, NIS2 sankcie
Iné náklady	5 %	PR kríza, zvýšené poistné

Zdroj: IBM Cost of a Data Breach Report 2024, vlastné spracovanie

Sektorové rozdiely v dopadoch

Náklady reputačných škôd sa významne líšia medzi sektormi. Najvyššie náklady na bezpečnostné incidenty sú konzistentne zaznamenávané v zdravotníctve, kde priemerný náklad dosahuje 10,93 milióna USD podľa IBM štúdie 2024, nasledované finančnými službami s 6,08 milióna USD a farmaceutickým priemyslom s 5,01 milióna USD.[37]

Tieto sektorové rozdiely odrážajú niekoľko faktorov. Ide o citlivosť spracovávaných dát, prísnosť regulačného rámca a výšku potenciálnych pokút a očakávania zákazníkov ohľadom bezpečnosti. Pre MSP pôsobiace v týchto vysoko citlivých sektoroch je investícia do bezpečnosti ešte kritickejšia.

Na druhej strane sektory s nižšími priemernými nákladmi, napríklad pohostinstvo alebo médiá, nemusia byť menej ohrozené, len majú rozdielnu štruktúru rizík. Pre MSP v týchto sektoroch môžu reputačné škody predstavovať proporcionálne vyšší dopad na ich menšiu zákaznícku základňu.

[37] **IBM Security.** *Cost of a Data Breach Report 2024.* Armonk, NY: IBM Corporation, 2024

4.3.4 Stratégie budovania dôvery pre MSP

Pre MSP existuje niekoľko praktických stratégií, ako transformovať regulačné požiadavky na nástroje budovania dôvery a reputácie. Tieto stratégie kombinujú formálne certifikácie s menej formálnymi, ale rovnako dôležitými prístupmi k transparentnosti a komunikácii.

Certifikácie a formálne preukazy súladu

Formálne certifikácie poskytujú nezávislý doklad o úrovni bezpečnosti a súladu, ktorý je zrozumiteľný pre zákazníkov a obchodných partnerov. Pre MSP sú relevantné najmä tieto certifikácie.

ISO/IEC 27001 je medzinárodný štandard pre systémy riadenia informačnej bezpečnosti (ISMS). Certifikácia podľa tohto štandardu preukazuje, že organizácia implementovala systematický prístup k riadeniu informačnej bezpečnosti. Pre MSP je získanie tejto certifikácie investíciou, ale často sa stáva nevyhnutnosťou pre spoluprácu s väčšími podnikmi a verejným sektorom.

SOC 2 (Service Organization Control 2) je rámec vyvinutý AICPA, ktorý je obzvlášť relevantný pre MSP poskytujúce cloudové služby alebo spracúvajúce dáta zákazníkov. SOC 2 reporty sú bežne vyžadované zákazníkmi v USA, ale ich význam rastie aj v Európe.

CE označenie podľa AI Act a CRA bude slúžiť ako formálny indikátor súladu pre produkty s digitálnymi prvkami a vysokorizikové AI systémy. Pre MSP vyvíjajúce takéto produkty bude CE označenie povinné a súčasne bude slúžiť ako marketingový nástroj preukazujúci splnenie európskych štandardov.

Sektorové certifikácie, ako napríklad ISO 13485 pre zdravotnícke prostriedky, PCI DSS pre spracovanie platobných kariet alebo certifikácie podľa schém ENISA pre cloudové služby, môžu byť relevantné pre MSP v špecifických odvetviach.

Transparentná komunikácia

Okrem formálnych certifikácií môžu MSP budovať dôveru prostredníctvom transparentnej komunikácie a aktívneho zapojenia so zákazníkmi a širšou verejnosťou. Konkrétne prístupy zahŕňajú niekoľko oblastí.

Publikovanie bezpečnostných politík na webovej stránke spoločnosti signalizuje zákazníkom, že bezpečnosť je prioritou. Politiky by mali byť napísané zrozumiteľným jazykom a pravidelne aktualizované.

Transparentnosť ohľadom AI je obzvlášť dôležitá pre MSP využívajúce alebo vyvíjajúce AI systémy. Zrozumiteľná komunikácia o tom, ako sú AI systémy využívané, aké dáta spracúvajú a aké rozhodnutia podporujú, buduje dôveru používateľov.

Reakcia na incidenty je kritickým momentom pre reputáciu. MSP by mali mať pripravený krízový komunikačný plán, ktorý zabezpečí rýchlu, transparentnú a empatickú komunikáciu

v prípade bezpečnostného incidentu. Spôsob, akým spoločnosť reaguje na krízu, často determinuje dlhodobý reputačný dopad viac než samotný incident.

Zapojenie zákazníkov do procesov súvisiacich s bezpečnosťou a etikou môže posilniť dôveru. Prístupy ako používateľské testovacie programy, poradné zbory zákazníkov pre otázky ochrany súkromia alebo transparentné mechanizmy spätnej väzby signalizujú, že spoločnosť počúva svojich zákazníkov.

Budovanie internej kultúry bezpečnosti

Dôveryhodnosť smerom navonok musí byť podložená skutočnou kultúrou bezpečnosti a etiky vo vnútri organizácie. Pre MSP to znamená zabezpečiť, že všetci zamestnanci rozumejú významu bezpečnosti a etiky a sú motivovaní prispievať k ich udržiavaniu.

Praktické kroky zahŕňajú pravidelné školenia pre všetkých zamestnancov, nielen IT, jasné procesy a zodpovednosti za bezpečnosť, pozitívne posilňovanie bezpečného správania, nielen sankcie za porušenia, otvorenú komunikáciu o bezpečnostných otázkach a incidentoch a zapojenie vedenia spoločnosti ako vzorov bezpečného správania.

Pre MSP s obmedzenými zdrojmi môže budovanie takejto kultúry predstavovať výzvu, ale súčasne aj príležitosť. Menšia veľkosť organizácie umožňuje priamu komunikáciu a rýchlejšie zakorenenie nových praktík než vo veľkých korporáciách s komplexnými hierarchiami.

4.3.5 Metriky a meranie reputačného kapitálu

Pre efektívne riadenie reputácie je potrebné ju merať. Hoci reputácia je nehmotné aktívum, existujú prístupy, ktoré MSP môžu využiť na sledovanie vývoja svojej dôveryhodnosti v očiach zákazníkov a partnerov.

Kľúčové ukazovatele dôvery zákazníkov

Medzi metriky, ktoré môžu MSP sledovať, patria napríklad Net Promoter Score (NPS), ktorý je štandardným nástrojom na meranie lojality a spokojnosti zákazníkov. Zmeny v NPS môžu indikovať posun vo vnímaní dôveryhodnosti.

Ďalej je to miera udržania zákazníkov (Customer Retention Rate), pričom pokles môže signalizovať problém s dôverou. Dôležitá je aj doba konverzie pri predaji. Dlhšia doba rozhodovania zákazníkov sa môže spájať s nedostatočnou dôverou.

Relevantné sú aj výsledky bezpečnostných auditov a dotazníkov. Zlepšujúce sa výsledky a pozitívna spätná väzba od zákazníkov potvrdzujú efektívnosť bezpečnostných investícií.

Monitorovanie mediálneho obrazu

Pre MSP môže byť užitočné sledovať aj to, ako sú vnímané v médiách a na sociálnych sieťach. Hoci MSP typicky nemajú kapacity na sofistikovaný média monitoring, základné sledovanie je možné aj s obmedzenými zdrojmi.

Google Alerts na názov spoločnosti a kľúčové produkty poskytuje bezplatný základný monitoring. Sledovanie zmienok na sociálnych sieťach môže odhaliť potenciálne problémy skôr. Dôležitý je aj pravidelný prehľad hodnotení a recenzií na relevantných platformách.

V prípade, že MSP čelí verejnej kritike alebo negatívnej publicite súvisiacej s bezpečnosťou alebo etikou, je dôležité reagovať rýchlo a profesionálne. Ignorovanie kritiky zriedka vedie k jej vymiznutiu, zatiaľ čo konštruktívna reakcia môže obrátiť negatívnu situáciu na príležitosť demonštrovať zodpovedný prístup.

4.3.6 Zhrnutie a odporúčania

Reputácia a dôvera zákazníkov sa stávajú kritickými faktormi úspechu v digitalizovanej ekonomike charakterizovanej rastúcimi obavami z kybernetických hrozieb a neetických praktík AI. Regulácie AI Act, CRA a NIS2 vytvárajú rámec, v ktorom MSP môžu budovať a preukázať svoju dôveryhodnosť.

Kľúčové zistenia

Kybernetická bezpečnosť sa transformovala z technickej záležitosti na strategický faktor ovplyvňujúci obchodné vzťahy. Až 72 % organizácií podstupuje bezpečnostné audity pre získanie zákaziek a 29 % stratilo kontrakt kvôli chýbajúcej certifikácii.

Náklady bezpečnostných incidentov sú pre MSP potenciálne existenčne ohrozujúce. Priemerné náklady 3,31 milióna USD pre menšie podniky a štatistika, že 60 % malých podnikov ukončí činnosť do šiestich mesiacov po útoku, ilustrujú kritickosť tejto problematiky.

Etický prístup k AI sa stáva hodnotovou propozíciou v prostredí rastúcich verejných obáv. Zakázané praktiky podľa AI Act odrážajú spoločenské očakávania, ktoré presahujú minimálne regulačné požiadavky.

Transparentnosť a aktívna komunikácia môžu MSP odlíšiť od veľkých korporácií, ktoré sú často vnímané ako netransparentné. Lokálne MSP majú príležitosť budovať dôveru prostredníctvom osobného prístupu.

Odporúčania pre MSP

Prvým odporúčaním je pristupovať k investíciám do bezpečnosti ako k strategickej investícii s merateľnou návratnosťou v podobe ochrany pred nákladmi incidentov a získania konkurenčnej výhody, nie ako k čistému nákladu.

Druhým odporúčaním je zvážiť získanie formálnych certifikácií, predovšetkým ISO 27001, ako nástroja na preukázanie bezpečnostnej zrelosti zákazníkom a partnerom a na diferenciáciu od konkurencie.

Tretím odporúčaním je budovať transparentnosť a otvorenú komunikáciu ako kľúčový prvok hodnotovej propozície, obzvlášť v oblasti AI, kde sú verejné obavy najvýraznejšie.

Štvrtým odporúčaním je pripraviť sa na krízovú komunikáciu, pretože spôsob reakcie na incident často determinuje dlhodobý reputačný dopad viac než samotný incident.

Piatym odporúčaním je budovať internú kultúru bezpečnosti a etiky, ktorá je základom dôveryhodnosti smerom navonok a ktorá zapája všetkých zamestnancov, nielen IT oddelenie.

Pre slovenské MSP platí, že v malom trhovom prostredí je reputácia obzvlášť cenná a zároveň zraniteľná. Negatívna skúsenosť jedného zákazníka sa môže rýchlo rozšíriť a poškodenie reputácie môže byť ťažšie napraviteľné než vo veľkých anonymných trhoch. Investície do bezpečnosti, etiky a transparentnosti sú preto pre slovenské MSP nie luxusom, ale strategickou nevyhnutnosťou.

4.4 Vplyv na dodávateľské reťazce

Moderné dodávateľské reťazce v oblasti digitálnych technológií sú charakterizované vysokou mierou prepojenosti a vzájomnej závislosti. Softvérové produkty typicky obsahujú desiatky až stovky komponentov od rôznych dodávateľov, hardvérové produkty integrujú čipy, moduly a firmware od globálnej siete výrobcov a poskytovatelia služieb sa spoliehajú na infraštruktúru a nástroje tretích strán. Táto komplexita vytvára riziká, ktoré regulácie AI Act, CRA a NIS2 explicitne adresujú prostredníctvom požiadaviek na bezpečnosť dodávateľských reťazcov.

Pre malé a stredné podniky má táto regulátorna pozornosť na dodávateľské reťazce dvojaký význam. Na jednej strane MSP pôsobiacim ako dodávatelia pre väčšie podniky vznikajú nové povinnosti preukazovať bezpečnosť a súlad, pretože ich odberatelia sú tlačení reguláciami na riadenie rizík v dodávateľskom reťazci. Na druhej strane MSP ako odberatelia musia zvažovať bezpečnosť svojich vlastných dodávateľov, čo môže vyžadovať zmeny v procese výberu a hodnotenia dodávateľov.

Táto podkapitola analyzuje regulatórne požiadavky na bezpečnosť dodávateľských reťazcov, empirické údaje o zraniteľnosti reťazcov a praktické dopady pre MSP v rôznych pozíciách v rámci dodávateľských vzťahov.

4.4.1 Kaskádová zodpovednosť v dodávateľskom reťazci podľa CRA

CRA zavádza koncept kaskádovej zodpovednosti, podľa ktorého výrobcovia finálnych produktov nesú zodpovednosť za bezpečnosť celého produktu vrátane komponentov od tretích strán. Tento prístup má za cieľ zabezpečiť, že bezpečnosť nebude obetovaná na oltár nákladovej efektívnosti pri rozhodovaniach o využití externých komponentov.

Právny rámec zodpovednosti podľa CRA

Podľa článku 13 CRA sú výrobcovia povinní zabezpečiť, že produkt s digitálnymi prvkami je navrhovaný, vyvíjaný a vyrábaný v súlade so základnými požiadavkami stanovenými v prílohe I nariadenia. Táto povinnosť sa vzťahuje na celý produkt vrátane všetkých integrovaných komponentov, a to bez ohľadu na to, či tieto komponenty pochádzajú od samotného výrobcu alebo od tretích strán.

Výrobca nemôže preniesť svoju zodpovednosť za bezpečnosť finálneho produktu na dodávateľov komponentov. Hoci môže zmluvne požadovať od dodávateľov určité bezpečnostné štandardy a môže mať právo na regres v prípade, že dodávateľ poruší zmluvné

podmienky, voči regulačným orgánom a koncovým používateľom zostáva zodpovedný výrobca finálneho produktu.

Pre MSP, ktoré sú výrobcami finálnych produktov, to znamená nevyhnutnosť dôkladného hodnotenia a riadenia bezpečnosti komponentov od tretích strán. Rozhodnutie využiť lacnejší komponent od menej etablovaného dodávateľa môže priniesť krátkodobé úspory, ale v prípade bezpečnostného problému bude náklady znášať výrobca, nie dodávateľ komponentu.

Povinnosti importérov a distribútorov

CRA definuje špecifické povinnosti aj pre importérov a distribútorov produktov s digitálnymi prvkami. Importéri (článok 19) musia zabezpečiť, že výrobca vykonal príslušné postupy posúdenia zhody a že produkt nesie CE označenie a je sprevádzaný požadovanou dokumentáciou. Ak má importér dôvod domnievať sa, že produkt nie je v súlade s požiadavkami, nesmie uvádzať produkt na trh, kým výrobca nezabezpečí nápravu.

Distribútori (článok 20) musia pred uvedením produktu na trh overiť, že produkt nesie CE označenie a je sprevádzaný požadovanou dokumentáciou a inštrukciami. Ak má distribútor dôvod domnievať sa, že produkt nie je v súlade, nesmie ho uvádzať na trh, kým nie je dosiahnutý súlad.

Pre MSP pôsobiace ako importéri alebo distribútori digitálnych produktov tieto povinnosti znamenajú potrebu due diligence[38] voči výrobcom a zavedenie procesov na overovanie súladnosti pred uvedením produktov na trh. Nedbanlivosť v tejto oblasti môže viesť k sankciám, aj keď samotná bezpečnostná chyba pochádza od výrobcu.

Tab. č. 14: **Rozloženie zodpovednosti v dodávateľskom reťazci podľa CRA**

Rola v reťazci	Hlavné povinnosti	Dopad pre MSP
Výrobca	Plná zodpovednosť za bezpečnosť produktu vrátane komponentov tretích strán, posúdenie zhody, CE označenie	Nutnosť riadiť bezpečnosť celého dodávateľského reťazca
Importér	Due diligence voči výrobcovi, overenie CE označenia a dokumentácie, neuvádzať nesúladný produkt	Procesy overovania pred importom
Distribútor	Overenie CE označenia a dokumentácie, nedistribuovať nesúladný produkt	Kontrola pred distribúciou
Dodávateľ komponentov	Zmluvné požiadavky od odberateľov, poskytovanie informácií o bezpečnosti	Zvýšené požiadavky od odberateľov

Zdroj: Nariadenie (EÚ) 2024/2847 (Cyber Resilience Act), články 13, 19, 20

[38] *Due diligence* je proces systematického preverovania právnych, finančných, technických a prevádzkových aspektov organizácie, projektu alebo obchodnej transakcie s cieľom identifikovať riziká, záväzky a potenciálne nedostatky pred prijatím rozhodnutia (napr. pred investíciou, akvizíciou alebo vstupom do zmluvného vzťahu). V kontexte regulácií EÚ môže zahŕňať aj preverovanie súladu s právnymi požiadavkami (compliance), najmä v oblasti ochrany údajov, kybernetickej bezpečnosti a riadenia rizík.

Software Bill of Materials (SBOM)

CRA v článku 13 ods. 5 zavádza požiadavku na vytváranie a udržiavanie SBOM pre produkty s digitálnymi prvkami. SBOM je formálny záznam obsahujúci detaily a vzťahy medzi komponentmi využitými pri stavbe softvéru. Tento koncept, inšpirovaný praxou v tradičnej výrobe, kde sú bežné kusovníky materiálov, umožňuje systematické sledovanie komponentov a identifikáciu zraniteľností.

Pre výrobcov to znamená povinnosť dokumentovať všetky softvérové komponenty využité v ich produktoch vrátane open-source knižníc, proprietárnych SDK od tretích strán, firmvéru a ďalších závislostí. SBOM musí byť udržiavaný aktuálny počas celého životného cyklu produktu a musí byť dostupný pre účely posúdenia zhody.

Praktickou implikáciou pre MSP je potreba zavedenia nástrojov a procesov pre automatizovanú tvorbu a správu SBOM. Pre malé vývojárske tímy to môže predstavovať výzvu, ale existujú open-source nástroje (napríklad SPDX, CycloneDX), ktoré môžu tento proces automatizovať a integrovať do existujúcich vývojárskych workflow.

4.4.2 NIS2 a bezpečnosť dodávateľského reťazca

Smernica NIS2 explicitne zahrňuje bezpečnosť dodávateľského reťazca medzi povinné opatrenia na riadenie kybernetických rizík. Článok 21 ods. 2 písmeno d stanovuje, že základné a dôležité subjekty musia implementovať opatrenia zahrnujúce bezpečnosť dodávateľského reťazca vrátane bezpečnostných aspektov týkajúcich sa vzťahov medzi každým subjektom a jeho priamymi dodávateľmi alebo poskytovateľmi služieb.

Rozsah povinností regulovaných subjektov

Regulované subjekty podľa NIS2 musia pri výbere dodávateľov a poskytovateľov služieb zohľadňovať ich bezpečnostné praktiky. To zahŕňa hodnotenie bezpečnosti potenciálnych dodávateľov pred uzavretím zmluvy, zahrnutie bezpečnostných požiadaviek do zmluvných podmienok, priebežný monitoring bezpečnostnej výkonnosti dodávateľov a reakciu na bezpečnostné incidenty týkajúce sa dodávateľov.

Rozsah týchto povinností sa vzťahuje na priamych dodávateľov a poskytovateľov služieb, pričom regulovaný subjekt musí pristupovať k riadeniu rizík primerane k významnosti dodávateľa a citlivosti dodávaných produktov alebo služieb. Kritické ICT služby a produkty si vyžadujú vyššiu úroveň due diligence ako komoditné služby s nízkym bezpečnostným významom.

Praktické implikácie pre MSP ako dodávateľov

Pre MSP dodávajúce produkty alebo služby subjektom regulovaným podľa NIS2 tieto požiadavky znamenajú, že môžu očakávať zvýšené požiadavky na preukázanie bezpečnosti od svojich odberateľov. Konkrétne formy týchto požiadaviek môžu zahŕňať bezpečnostné dotazníky a audity, kde veľkí odberatelia zasielajú detailné dotazníky o bezpečnostných praktikách a môžu požadovať právo auditu. Ďalej zmluvné bezpečnostné klauzuly, kde zmluvy obsahujú špecifické bezpečnostné požiadavky so sankciami za nedodržanie.

Taktiež požiadavky na certifikácie, kde odberatelia môžu požadovať certifikácie ako ISO 27001 ako podmienku spolupráce. A napokon procesy oznamovania incidentov, kde zmluvy môžu stanovovať povinnosť oznamovať bezpečnostné incidenty odberateľovi v stanovených lehotách.

Pre MSP, ktoré doteraz nemali formalizované bezpečnostné procesy, môžu tieto požiadavky predstavovať významnú záťaž. Na druhej strane MSP, ktoré už majú zavedené bezpečnostné praktiky a certifikácie, môžu tieto požiadavky využiť ako konkurenčnú výhodu pri získavaní zákaziek od regulovaných subjektov.

Tab. č. 15: **Typické bezpečnostné požiadavky na dodávateľov od NIS2 regulovaných subjektov**

Typ požiadavky	Popis	Úroveň záťaže pre MSP
Bezpečnostný dotazník	Vyplnenie štandardizovaného dotazníka o bezpečnostných praktikách	Nízka až stredná
Právo na audit	Umožnenie auditu bezpečnostných praktik odberateľom	Stredná
Certifikácia ISO 27001	Požiadavka na certifikovaný ISMS	Vysoká
Zmluvné SLA pre bezpečnosť	Špecifické metriky a záväzky v oblasti bezpečnosti	Stredná
Notifikácia incidentov	Povinnosť hlásiť incidenty v stanovených lehotách	Nízka
Penetračné testovanie	Pravidelné testovanie produktov/služieb treťou stranou	Stredná až vysoká

Zdroj: Vlastné spracovanie na základe požiadaviek NIS2 a trhovej praxe

4.4.3 Empirické údaje o zraniteľnosti dodávateľských reťazcov

Regulátorna pozornosť na bezpečnosť dodávateľských reťazcov reflektuje reálne hrozby dokumentované v empirických štúdiách a bezpečnostných incidentoch. Útoky na dodávateľské reťazce sa stali jedným z najvýznamnejších vektorov kybernetických hrozieb, pretože umožňujú útočníkom zasiahnuť veľký počet obetí prostredníctvom kompromitácie jedného dodávateľa.

Štatistiky o útokoch na dodávateľské reťazce

Podľa správy ENISA Threat Landscape 2024 došlo k 400% nárastu útokov na dodávateľské reťazce v porovnaní s rokom 2020. Tento dramatický nárast odráža strategický posun útočníkov smerom k cieleniu na dodávateľské reťazce ako efektívnejší spôsob zasiahnuť veľký počet obetí.

Verizon Data Breach Investigations Report 2024 uvádza, že tretie strany boli priamo zapojené do 15 % všetkých analyzovaných bezpečnostných incidentov, pričom v niektorých sektoroch (napríklad finančné služby) je tento podiel ešte vyšší. Incidenty zahŕňajúce

dodávateľský reťazec majú typicky tiež závažnejšie dopady, pretože zasahujú viaceré organizácie súčasne.[39]

Štúdia Ponemon Institute z roku 2024 zistila, že 54 % organizácií zažilo bezpečnostný incident spôsobený treťou stranou v posledných 12 mesiacoch. Priemerné náklady na incident spôsobený treťou stranou dosahovali 4,29 milióna USD, čo je porovnateľné s priemerným bezpečnostným incidentom.[40]

Tab. č. 16: **Štatistiky o bezpečnostných incidentoch v dodávateľských reťazcoch**

Indikátor	Hodnota	Zdroj
Nárast útokov na supply chain od 2020	400 %	ENISA 2024
Podiel incidentov zahrnujúcich tretiu stranu	15 %	Verizon DBIR 2024
Organizácie s incidentom od tretej strany (12 mes.)	54 %	Ponemon 2024
Priemerné náklady incidentu od tretej strany	4,29 mil. USD	Ponemon 2024
Organizácie bez plánu reakcie na supply chain incident	41 %	Gartner 2024
Priemerný počet tretích strán s prístupom k dátam	89	SecurityScorecard

Zdroj: ENISA Threat Landscape 2024, Verizon DBIR 2024, Ponemon Institute, Gartner, SecurityScorecard

Významné incidenty a ich poučenia

Incident SolarWinds z roku 2020 zostáva referenčným prípadom útoku na dodávateľský reťazec. Útočníci kompromitovali build systém spoločnosti SolarWinds a vložili malware do aktualizácií softvéru Orion, ktorý využívalo viac ako 18 000 organizácií vrátane vládnych agentúr a veľkých korporácií. Incident ilustroval, ako kompromitácia jedného dodávateľa môže poskytnúť prístup k tisíckam organizácií.[41]

Útok na Kaseya v roku 2021 zasiahol prostredníctvom softvéru pre správu IT infraštruktúry až 1 500 koncových organizácií. Útočníci využili zraniteľnosť v softvéri Kaseya VSA na distribúciu ransomware k zákazníkom spravovaným poskytovateľmi služieb využívajúcimi tento softvér.[42]

Incident Log4j v roku 2021 odhalil riziko závislosti na open-source komponentoch. Kritická zraniteľnosť v široko využívanej knižnici Log4j zasiahla milióny aplikácií a systémov

[39] V**erizon.** *2024 Data Breach Investigations Report (DBIR).* New York: Verizon Enterprise, 2024
[40] **Ponemon Institute.** *Cost of a Data Breach Report 2024.* Research report conducted by Ponemon Institute and sponsored by IBM Security, 2024
[41] **U.S. Cybersecurity and Infrastructure Security Agency (CISA).** *Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations (SolarWinds Supply Chain Compromise).* Washington, D.C., 2020
[42] **National Institute of Standards and Technology (NIST).** *NIST Vulnerability Note VU#930724 – Apache Log4j2 Remote Code Execution Vulnerability.* Gaithersburg, MD, 2021

po celom svete. Mnohé organizácie nemali prehľad o tom, kde všade využívajú Log4j, čo sťažovalo reakciu na zraniteľnosť.

Pre MSP tieto incidenty ilustrujú niekoľko kľúčových poučení. Po prvé, aj malý dodávateľ môže byť vstupným bodom pre útok na veľké organizácie, čo zvyšuje atraktivitu MSP ako cieľov. Po druhé, viditeľnosť do vlastného dodávateľského reťazca (vedieť, aké komponenty využívam) je kritická pre schopnosť reagovať na zraniteľnosti. Po tretie, bezpečnostné praktiky dodávateľov majú priamy dopad na bezpečnosť odberateľov.

Open-source závislosti a ich riziká

Moderný softvérový vývoj sa vo veľkej miere spolieha na open-source komponenty. Podľa štúdií až 90 % moderných aplikácií obsahuje open-source kód a priemerná aplikácia má desiatky až stovky priamych a nepriamych závislostí na open-source knižniciach. Tento model prináša významné výhody v podobe urýchlenia vývoja a zdieľania nákladov, ale tiež vytvára riziká.

Open-source projekty sú často udržiavané malým počtom dobrovoľníkov bez formálnych bezpečnostných procesov. Zraniteľnosti môžu zostať neopravené dlhší čas a organizácie využívajúce tieto komponenty nemusia mať prehľad o tom, aké zraniteľnosti sa ich týkajú.

CRA adresuje tieto riziká požiadavkou na SBOM a povinnosťou výrobcov monitorovať a opravovať zraniteľnosti v ich produktoch vrátane open-source komponentov. Pre MSP to znamená potrebu zavedenia procesov na sledovanie open-source závislostí, monitorovanie zraniteľností a včasnú aplikáciu opráv.

4.4.4 Praktické dôsledky pre MSP v dodávateľských reťazcoch

Na základe regulatórnych požiadaviek a empirických údajov o rizikách možno identifikovať konkrétne praktické dôsledky pre MSP v rôznych pozíciách v rámci dodávateľských reťazcov.

MSP ako dodávatelia pre veľké podniky

MSP dodávajúce produkty alebo služby veľkým podnikom, najmä tým, ktoré podliehajú reguláciám NIS2, DORA alebo sektorovým predpisom, musia očakávať rastúce požiadavky na preukázanie bezpečnostných praktík. Praktické kroky zahŕňajú prípravu na bezpečnostné due diligence, kde je potrebné mať pripravené odpovede na štandardné bezpečnostné dotazníky, dokumentáciu bezpečnostných politík a procesov a doklady o bezpečnostných opatreniach.

Ďalej je vhodné zvážiť formálnu certifikáciu, pričom ISO 27001 sa stáva de facto štandardom, ktorý odberatelia očakávajú, a certifikácia zjednodušuje proces due diligence a buduje dôveru. Potrebné je tiež implementovať procesy pre reakciu na incidenty vrátane schopnosti rýchlo reagovať a komunikovať v prípade bezpečnostného incidentu, mať pripravený „*incident response*“ plán a komunikačné kanály k odberateľom. V neposlednom rade je nutné monitorovať vlastné závislosti a mať prehľad o komponentoch tretích strán využitých vo vlastných produktoch a schopnosť reagovať na zraniteľnosti.

MSP ako výrobcovia produktov

Pre MSP vyrábajúce produkty s digitálnymi prvkami podliehajúce CRA vznikajú špecifické povinnosti súvisiace s dodávateľským reťazcom. Predovšetkým je to due diligence voči dodávateľom komponentov, čo znamená hodnotenie bezpečnostných praktík dodávateľov pred začatím spolupráce, overovanie súladu dodávaných komponentov s bezpečnostnými požiadavkami a zmluvné zabezpečenie práva na informácie o zraniteľnostiach.

Ďalej je potrebné vytváranie a správa SBOM pre všetky produkty, využitie nástrojov na automatizovanú tvorbu SBOM, integrácia SBOM do vývojových procesov (CI/CD pipeline) a pravidelná aktualizácia SBOM počas životného cyklu produktu. Rovnako dôležité je monitorovanie zraniteľností v komponentoch prostredníctvom sledovania bezpečnostných bulletinov a databáz zraniteľností (CVE) pre využívané komponenty, hodnotenie dopadu zraniteľností na vlastné produkty a včasná distribúcia opráv koncovým používateľom.

MSP ako poskytovatelia IT služieb

Malé a stredné podniky poskytujúce IT služby, napríklad managed services, cloud hosting alebo vývoj softvéru na zákazku, sa často nachádzajú v postavení, v ktorom majú privilegovaný prístup k systémom a údajom svojich zákazníkov. Z tohto dôvodu na ne prirodzene dopadajú vyššie nároky na bezpečnosť a zároveň možno zo strany zákazníkov očakávať prísnejšie bezpečnostné požiadavky.

V praxi to znamená najmä potrebu dôsledne oddeliť jednotlivé zákaznícke prostredia tak, aby bezpečnostný incident u jedného zákazníka neohrozil ostatných. Rovnako je nevyhnutné zabezpečiť bezpečný vzdialený prístup k zákazníckym systémom, a to s využitím silnej autentifikácie, šifrovania a zaznamenávania prístupov.

Dôležitou oblasťou je aj správa privilegovaných účtov, ktorá zahŕňa prísnu kontrolu administrátorských oprávnení a uplatňovanie princípu minimálnych oprávnení. Nevyhnutnou súčasťou poskytovania IT služieb je napokon aj zabezpečenie kontinuity činnosti a obnovy, teda schopnosť pokračovať v poskytovaní služieb a v prípade incidentu obnoviť prevádzku a funkčnosť zákazníckych systémov.

Tab. č. 17: **Odporúčania pre MSP podľa pozície v dodávateľskom reťazci**

Pozícia MSP	Prioritné opatrenia	Investičná náročnosť
Dodávateľ pre veľké podniky	Certifikácia ISO 27001, dokumentované politiky, incident response plán	Stredná až vysoká (certifikácia)
Výrobca produktov (CRA)	SBOM nástroje, due diligence dodávateľov, CVE monitoring	Stredná (nástroje a procesy)
Poskytovateľ IT služieb	Segregácia prostredí, PAM, bezpečný vzdialený prístup	Stredná (infraštruktúra)
SW vývojár (subdodávateľ)	Secure SDLC, code review, bezpečné vývojové prostredie	Nízka až stredná (procesy)
Distribútor/reseller	Due diligence výrobcov, overovanie CE označenia a dokumentácie	Nízka (procesy)

Zdroj: Vlastné spracovanie na základe požiadaviek CRA, NIS2 a trhovej praxe

4.4.5 Strategické odpovede na reguláciu dodávateľských reťazcov

MSP môžu na rastúce požiadavky v oblasti bezpečnosti dodávateľských reťazcov reagovať rôznymi strategickými prístupmi. Výber vhodnej stratégie závisí od pozície MSP v hodnotovom reťazci, zdrojov a ambícií.

Proaktívna diferenciácia

Niektoré MSP môžu zvoliť stratégiu proaktívnej diferenciácie, kde bezpečnosť dodávateľského reťazca využijú ako konkurenčnú výhodu. Táto stratégia zahŕňa investície do bezpečnosti presahujúce minimálne požiadavky, získanie pokročilých certifikácií a budovanie reputácie dôveryhodného partnera.

Výhody tohto prístupu zahŕňajú schopnosť účtovať prémiovú cenu za služby, preferenciu zo strany náročných zákazníkov a odolnosť voči cenovej konkurencii. Nevýhodou sú vyššie počiatočné investície a potreba kontinuálneho udržiavania vedúcej pozície.

Reaktívna adaptácia

Alternatívnym prístupom je reaktívna adaptácia, kde MSP implementuje bezpečnostné opatrenia v rozsahu požadovanom zákazníkmi a reguláciami, bez ambície presiahnuť minimálne požiadavky. Táto stratégia minimalizuje investície, ale nesie riziko straty zákazníkov, ak konkurenti ponúknu vyššiu úroveň bezpečnosti.

Pre mnohé MSP s obmedzenými zdrojmi môže byť tento prístup realistickou východiskovou pozíciou s možnosťou postupného zvyšovania úrovne bezpečnosti podľa vývoja trhu a dostupných zdrojov.

Špecializácia a partnerstvá

Treťou stratégiou je špecializácia na konkrétnu oblasť a budovanie partnerstiev pre doplňanie chýbajúcich kompetencií. MSP sa môže sústrediť na svoju hlavnú odbornosť a pre bezpečnostné aspekty spolupracovať so špecializovanými partnermi.

Tento prístup môže zahŕňať outsourcing bezpečnostného monitoringu na managed security service providera (MSSP), využitie bezpečnostných nástrojov ako služby (Security-as-a-Service), partnerstvo s konzultačnou firmou pre audity a certifikácie alebo účasť v sektorových iniciatívach pre zdieľanie informácií o hrozbách.

4.4.6 Zhrnutie a kľúčové závery

Regulácie AI Act, CRA a NIS2 prinášajú zásadnú zmenu v prístupe k bezpečnosti dodávateľských reťazcov. Kaskádová zodpovednosť, požiadavky na SBOM a povinnosť riadiť riziká tretích strán vytvárajú nové povinnosti pre MSP vo všetkých pozíciách dodávateľského reťazca.

Kľúčové zistenia

Výrobcovia nesú plnú zodpovednosť za bezpečnosť produktov vrátane komponentov od tretích strán. Pre MSP vyrábajúce produkty s digitálnymi prvkami to znamená nevyhnutnosť due diligence voči dodávateľom a systematického riadenia bezpečnosti komponentov.

Regulované subjekty podľa NIS2 prenášajú bezpečnostné požiadavky na svojich dodávateľov. MSP dodávajúce pre veľké podniky a verejný sektor môžu očakávať rastúce požiadavky na certifikácie, audity a bezpečnostné záväzky.

Útoky na dodávateľské reťazce dramaticky narastajú (400 % od roku 2020). Pre MSP to znamená, že sú potenciálnymi cieľmi útokov aj vtedy, ak priamo nespravujú cenné aktíva, pretože môžu slúžiť ako vstupný bod k väčším organizáciám.

SBOM sa stáva povinným nástrojom pre sledovanie komponentov a riadenie zraniteľností. MSP vyvíjajúce softvér musia implementovať nástroje a procesy pre automatizovanú tvorbu a správu SBOM.

Odporúčania pre slovenské MSP

Slovenské MSP by mali zmapovať svoju pozíciu v dodávateľských reťazcoch a identifikovať, ktorí ich odberatelia podliehajú reguláciám NIS2, CRA alebo sektorovým predpisom a aké požiadavky z toho vyplývajú.

Ďalej by mali zaviesť základné procesy riadenia bezpečnosti dodávateľského reťazca vrátane hodnotenia dodávateľov, zmluvných bezpečnostných klauzúl a monitorovania zraniteľností v externých komponentoch.

Mali by tiež pripraviť sa na zvýšené požiadavky od odberateľov prostredníctvom dokumentácie bezpečnostných praktík, prípravy na bezpečnostné dotazníky a zváženia formálnej certifikácie.

Pre MSP vo výrobe produktov s digitálnymi prvkami je potrebné implementovať nástroje pre SBOM a integrovať bezpečnosť do vývojového procesu (Security by Design, DevSecOps).

Napokon by mali zvážiť partnerstvá a zdieľané zdroje, pretože spolupráca s inými MSP, využitie managed security services a účasť v sektorových iniciatívach môžu pomôcť prekonať obmedzenia vlastných kapacít.

Bezpečnosť dodávateľského reťazca sa stáva nevyhnutnou súčasťou podnikania v digitálnej ekonomike. MSP, ktoré túto realitu akceptujú a proaktívne na ňu reagujú, môžu transformovať regulačnú záťaž na konkurenčnú výhodu a posilniť svoju pozíciu v dodávateľských vzťahoch s väčšími partnermi.

4.5 Strategické dôsledky pre MSP

Analýza nepriamych dopadov technologických regulácií EÚ na malé a stredné podniky odhaľuje komplexnú krajinu príležitostí a hrozieb, ktorá si vyžaduje strategický prístup. MSP nemôžu pristupovať k reguláciám AI Act, CRA a NIS2 ako k izolovaným compliance projektom, ale musia ich integrovať do celkovej podnikovej stratégie. Táto podkapitola syntetizuje zistenia predchádzajúcich častí a formuluje strategický rámec pre rozhodovanie MSP v novom regulačnom prostredí.

Strategická odpoveď na regulácie sa bude líšiť v závislosti od typu MSP, jeho pozície v hodnotovom reťazci, sektora pôsobnosti a dostupných zdrojov. Neexistuje univerzálne riešenie vhodné pre všetky MSP. Namiesto toho je potrebné, aby každé MSP vykonalo vlastnú strategickú analýzu a zvolilo prístup zodpovedajúci jeho špecifickej situácii.

Cieľom tejto podkapitoly je poskytnúť analytický rámec a praktické nástroje, ktoré MSP môžu využiť pri formulácii vlastnej stratégie. Podkapitola identifikuje typové strategické pozície, analyzuje faktory ovplyvňujúce voľbu stratégie a poskytuje odporúčania pre implementáciu.

4.5.1 Typológia strategických pozícií MSP

Na základe analýzy dopadov regulácií a charakteristík MSP možno identifikovať niekoľko typových strategických pozícií, ktoré MSP môžu zaujať voči novému regulačnému prostrediu. Tieto pozície predstavujú idealotypy a v praxi môže konkrétne MSP kombinovať prvky viacerých pozícií.

1. **Pozícia 1: Regulačný líder**

Regulačný líder je MSP, ktoré sa rozhodne pristupovať k reguláciám proaktívne a využiť ich ako zdroj konkurenčnej výhody. Táto pozícia je vhodná pre MSP s ambíciou rastu, dostatočnými zdrojmi na investície do compliance a pôsobením v sektoroch, kde zákazníci vysoko hodnotia bezpečnosť a dôveryhodnosť.

Charakteristiky regulačného lídra zahŕňajú investície do compliance presahujúce minimálne požiadavky, získanie pokročilých certifikácií (ISO 27001, SOC 2) skôr, ako ich zákazníci explicitne vyžadujú, aktívnu komunikáciu bezpečnostných a etických záväzkov ako súčasti brand identity, účasť v regulačných sandboxoch a pilotných projektoch a budovanie expertízy, ktorú možno monetizovať prostredníctvom konzultačných služieb.

Výhody tejto pozície zahŕňajú schopnosť účtovať prémiové ceny, preferenciu zo strany náročných zákazníkov, odolnosť voči cenovej konkurencii a príležitosť na diverzifikáciu príjmov prostredníctvom compliance služieb. Riziká zahŕňajú vysoké počiatočné investície, potrebu kontinuálneho udržiavania vedúcej pozície a možnosť, že trh nebude dostatočne oceňovať nadštandardnú úroveň compliance.

2. Pozícia 2: Rýchly nasledovník

Rýchly nasledovník je MSP, ktoré pozorne sleduje vývoj regulácií a trhu a implementuje potrebné opatrenia včas, ale bez ambície byť lídrom. Táto pozícia je vhodná pre MSP s obmedzenými zdrojmi, ktoré však pôsobia v prostredí, kde compliance bude čoskoro nevyhnutnosťou.

Charakteristiky rýchleho nasledovníka zahŕňajú systematický monitoring regulačného vývoja a požiadaviek zákazníkov, implementáciu compliance opatrení v dostatočnom predstihu pred deadlinami, využívanie skúseností a best practices od lídrov a regulátorov, efektívne alokovanie zdrojov na najnutnejšie opatrenia a pripravenosť rýchlo reagovať na zmeny požiadaviek.

Výhody tejto pozície zahŕňajú nižšie investície ako u lídra, možnosť učiť sa z chýb priekopníkov, flexibilitu pri adaptácii na meniace sa požiadavky a zachovanie konkurencieschopnosti bez nadmerných nákladov. Riziká zahŕňajú možnosť oneskorenia a strát zákaziek v prechodnom období, závislosť na dostupnosti informácií a best practices a nižší diferenciačný potenciál.

3. Pozícia 3: Minimalistický adaptér

Minimalistický adaptér je MSP, ktoré implementuje len nevyhnutné minimum požadované reguláciami a zákazníkmi. Táto pozícia môže byť realitou pre MSP s veľmi obmedzenými zdrojmi alebo pôsobiace v sektoroch s nízkym regulačným dopadom.

Charakteristiky minimalistického adaptéra zahŕňajú implementáciu len povinných požiadaviek, reaktívny prístup riadený externými tlakmi, minimalizáciu investícií do compliance, spoliehanie sa na výnimky a prechodné obdobia a prioritizáciu prežitia pred rastom.

Výhody tejto pozície zahŕňajú najnižšie krátkodobé náklady a zachovanie zdrojov pre iné priority. Riziká sú však významné a zahŕňajú stratu zákazníkov vyžadujúcich vyššiu úroveň compliance, neschopnosť reagovať na náhle zmeny požiadaviek, reputačné riziká v prípade incidentu a dlhodobú neudržateľnosť v regulovaných sektoroch.

4. Pozícia 4: Strategický exiter

Strategický exiter je MSP, ktoré po analýze regulačných dopadov dospeje k záveru, že náklady na compliance prevyšujú očakávané prínosy a rozhodne sa opustiť regulované oblasti pôsobenia. Táto pozícia môže byť racionálna pre MSP, ktorých hlavné aktivity sú mimo regulovaného rozsahu alebo ktorých obchodný model sa stáva neudržateľným.

Charakteristiky strategického exitera zahŕňajú dôkladnú analýzu nákladov a prínosov compliance, identifikáciu alternatívnych trhových príležitostí mimo regulovaného rozsahu, riadený prechod k novým aktivitám a minimalizáciu strát z opustenia existujúcich aktivít.

Výhody tejto pozície zahŕňajú vyhnutie sa nákladom compliance a možnosť sústrediť zdroje na perspektívnejšie oblasti. Riziká zahŕňajú stratu existujúcich zákazníkov a trhovej

pozície, náklady na prechod k novým aktivitám a možnosť, že regulácie sa rozšíria aj do nových oblastí pôsobenia.

Tab. č. 18: **Porovnanie strategických pozícií MSP**

Kritérium	Regulačný líder	Rýchly nasledovník	Minimalist. adaptér	Strategický exiter
Investície	Vysoké	Stredné	Nízke	Do prechodu
Časový horizont	Dlhodobý	Strednodobý	Krátkodobý	Jednorazový
Rizikový profil	Stredné	Nízke	Vysoké	Špecifické
Rastový potenciál	Vysoký	Stredný	Obmedzený	V novej oblasti
Vhodné pre	Ambiciózne MSP	Väčšinu MSP	Marginálne MSP	MSP mimo jadra

Zdroj: Vlastné spracovanie

4.5.2 Faktory ovplyvňujúce voľbu strategickej pozície

Voľba vhodnej strategickej pozície závisí od radu faktorov špecifických pre každé MSP. Systematická analýza týchto faktorov je predpokladom informovaného strategického rozhodnutia.

Miera regulačnej expozície

Prvý a najdôležitejší faktor je miera, do akej sú aktivity MSP priamo regulované novými predpismi. MSP vyvíjajúce vysokorizikové AI systémy podľa AI Act, vyrábajúce produkty s digitálnymi prvkami podľa CRA alebo pôsobiace v sektoroch regulovaných NIS2 majú vysokú regulačnú expozíciu a musia zvoliť aktívnejší prístup (líder alebo rýchly nasledovník).

Naopak, MSP, ktorých aktivity sú mimo priameho rozsahu regulácií (napríklad poskytovatelia profesionálnych služieb nevyužívajúci AI, remeselnícke podniky bez digitálnych produktov), majú nízku priamu expozíciu. Aj tieto MSP však môžu byť nepriamo ovplyvnené prostredníctvom požiadaviek zákazníkov alebo dodávateľov.

Pozícia v hodnotovom reťazci

Pozícia MSP v hodnotovom reťazci určuje, či bude MSP primárne nositeľom compliance povinností alebo príjemcom požiadaviek od iných. Výrobcovia finálnych produktov (CRA) a poskytovatelia služieb priamo regulovaným subjektom (NIS2) nesú priame povinnosti. Dodávatelia komponentov a subdodávatelia sú ovplyvnení nepriamo prostredníctvom požiadaviek odberateľov.

Pre MSP v strede hodnotového reťazca je kľúčové pochopiť požiadavky z oboch smerov – od regulátorov aj od zákazníkov – a nájsť efektívny spôsob ich plnenia. Synergický prístup, ktorý jednou sadou opatrení uspokojí viaceré požiadavky, je nákladovo efektívnejší než paralelné riešenia.

Sektorová dynamika

Rôzne sektory sa líšia v intenzite regulačného dopadu a v očakávaniach zákazníkov. V sektoroch ako finančné služby, zdravotníctvo alebo kritická infraštruktúra je regulačná expozícia vysoká a zákazníci očakávajú nadštandardnú úroveň bezpečnosti. V týchto sektoroch je pozícia lídra alebo rýchleho nasledovníka prakticky nevyhnutná.

V sektoroch s nižšou regulačnou intenzitou (napríklad retailové služby, pohostinstvo) môže byť pozícia minimalistického adaptéra krátkodobo udržateľná. Dlhodobo však treba očakávať rozširovanie regulačných požiadaviek a zvyšovanie očakávaní zákazníkov aj v týchto sektoroch.

Zdrojová vybavenosť

Dostupnosť finančných, ľudských a technických zdrojov limituje možnosti strategickej voľby. MSP s obmedzenými zdrojmi nemôže realisticky aspirovať na pozíciu lídra, ktorá vyžaduje významné investície. Pre takéto MSP je prioritou efektívne využitie dostupných zdrojov a maximálne využitie externej podpory (EDIH, granty, zdieľané služby).

Na druhej strane, MSP s dostatočnými zdrojmi, ktoré sa rozhodne pre minimalistický prístup, môže premrhať príležitosť na budovanie konkurenčnej výhody a dlhodobo oslabiť svoju pozíciu.

Strategické ambície

Strategické ambície manažmentu a vlastníkov ovplyvňujú voľbu pozície. MSP s ambíciou rastu, medzinárodnej expanzie alebo akvizičnej atraktivity bude prirodzene inklinovať k aktívnejšiemu prístupu k compliance. MSP orientované na stabilitu a udržanie existujúcej pozície môže zvoliť konzervatívnejší prístup.

Dôležité je, aby zvolená strategická pozícia bola v súlade s celkovou podnikovou stratégiou a aby compliance stratégia bola komunikovaná a zdieľaná naprieč celou organizáciou.

Tab. č. 19: **Faktory ovplyvňujúce voľbu strategickej pozície**

Faktor	Nízka hodnota	Vysoká hodnota	Implikácia
Regulačná expozícia	Mimo rozsahu regulácií	Priame povinnosti	Vysoká -> aktívny prístup
Pozícia v reťazci	Koncový dodávateľ	Výrobca, integrátor	Integrátor -> vyššie požiadavky
Sektorová dynamika	Nízka citlivosť	Regulovaný sektor	Citlivý -> vyššie očakávania
Dostupné zdroje	Obmedzené	Dostatočné	Zdroje -> možnosti investícií
Strategické ambície	Stabilita	Rast, expanzia	Ambície -> aktívnejší prístup

Zdroj: Vlastné spracovanie

4.5.3 Implementačný rámec pre strategickú odpoveď

Po zvolení strategickej pozície nasleduje fáza implementácie. Nasledujúci rámec poskytuje štruktúru pre systematickú implementáciu strategickej odpovede na regulácie.

Fáza 1: Diagnostika a hodnotenie

Prvá fáza zahŕňa dôkladnú diagnostiku súčasného stavu a hodnotenie regulačných požiadaviek. Konkrétne aktivity zahŕňajú:

- mapovanie regulačnej expozície, teda identifikáciu, ktoré regulácie sa vzťahujú na aktivity MSP a v akom rozsahu,
- gap analýzu, čo je porovnanie súčasného stavu s požiadavkami regulácií a identifikácia oblastí vyžadujúcich zlepšenie,
- hodnotenie rizík, čo je analýza pravdepodobnosti a dopadu nesúladu pre jednotlivé oblasti
- inventarizáciu zdrojov, teda prehľad dostupných finančných, ľudských a technických zdrojov pre compliance aktivity.

Výstupom tejto fázy by mal byť dokument sumarizujúci regulačnú expozíciu, identifikované medzery a priority pre ďalšie kroky.

Fáza 2: Plánovanie a príprava

Druhá fáza zahŕňa plánovanie konkrétnych opatrení a prípravu na implementáciu. Aktivity zahŕňajú vypracovanie compliance roadmapy, teda časový plán implementácie jednotlivých opatrení s priradením zodpovedností a zdrojov. Ďalej rozpočtovanie, čiže alokáciu finančných zdrojov na compliance aktivity vrátane rezervy na nepredvídané náklady. Tiež výber partnerov a dodávateľov, teda identifikáciu externých partnerov pre oblasti, kde MSP nemá interné kapacity (konzultanti, audítori, technológie), a prípravu internej komunikácie, teda plán komunikácie compliance stratégie zamestnancom a získanie ich buy-in.

Kľúčové je, aby plán bol realistický vzhľadom na dostupné zdroje a aby obsahoval jasné míľniky pre sledovanie pokroku.

Fáza 3: Implementácia

Tretia fáza je samotná implementácia plánovaných opatrení. Typické aktivity podľa oblasti zahŕňajú technické opatrenia, ako implementáciu bezpečnostných technológií, úpravu produktov, zavedenie SBOM nástrojov, procesné opatrenia, ako formalizáciu politík a procedúr, zavedenie procesov riadenia rizík a incident response, organizačné opatrenia, ako definovanie rolí a zodpovedností a prípadné zriadenie špecializovaných pozícií (DPO, CISO), a napokon oblasť ľudských zdrojov, teda školenie zamestnancov a prípadne nábor špecializovaných kompetencií.

Implementácia by mala prebiehať iteratívne s pravidelným vyhodnocovaním pokroku a úpravou plánu podľa potreby.

Fáza 4: Certifikácia a validácia

Štvrtá fáza zahŕňa formálne overenie súladu prostredníctvom certifikácie alebo inej formy validácie. Aktivity môžu zahŕňať internú validáciu, teda interný audit a testovanie implementovaných opatrení pred externým hodnotením, výber certifikačného orgánu, čiže výber akreditovaného orgánu pre príslušnú certifikáciu (ISO 27001, CE posúdenie zhody), samotný certifikačný audit a napokon nápravu zistení, teda adresovanie prípadných nezhôd identifikovaných počas auditu.

Pre MSP voliace pozíciu lídra alebo rýchleho nasledovníka je formálna certifikácia dôležitým míľnikom a nástrojom komunikácie voči zákazníkom.

Fáza 5: Udržiavanie a kontinuálne zlepšovanie

Piata fáza je kontinuálna a zahŕňa udržiavanie dosiahnutého stavu a neustále zlepšovanie. Aktivity zahŕňajú pravidelné interné audity a self-assessment, recertifikačné audity (typicky ročne pre ISO 27001), monitoring regulačného vývoja a adaptáciu na zmeny, sledovanie bezpečnostných hrozieb a aktualizáciu opatrení a pravidelné školenia a zvyšovanie povedomia zamestnancov.

Compliance nie je jednorazový projekt, ale kontinuálny proces. MSP musia alokovať zdroje na dlhodobé udržiavanie a zlepšovanie compliance programu.

4.5.4 Praktické nástroje a zdroje podpory

Implementácia strategickej odpovede na regulácie vyžaduje využitie rôznych nástrojov a zdrojov podpory. Pre MSP s obmedzenými internými kapacitami je efektívne využitie externých zdrojov kľúčové.

Európske podporné nástroje

Európska únia poskytuje komplexnú infraštruktúru podpory pre MSP v oblasti digitálnej transformácie a compliance. Medzi kľúčové nástroje patria Európske centrá digitálnych inovácií, ktoré poskytujú bezplatné alebo dotované služby vrátane testovania technológií, školení, poradenstva a networkingu, pričom od roku 2025 fungujú aj ako AI helpdesky pre otázky súvisiace s AI Act.

Ďalším nástrojom sú regulačné sandboxy, ktoré poskytujú bezpečné prostredie pre testovanie inovatívnych AI systémov s prioritným prístupom a ochranou pred pokutami pre MSP. Dokumentácia zo sandboxu môže slúžiť ako dôkaz súladu. Zariadenia pre testovanie a experimentovanie (TEFs) poskytujú prístup k špičkovej infraštruktúre pre sektorové testovanie AI a digitálnych technológií.

Grantové programy ako Horizont Europe, Digital Europe, Nástroj pre prepájanie Európy (CEF) – Digital, InvestEU a Fond obnovy a odolnosti ponúkajú financovanie projektov v oblasti digitalizácie a kybernetickej bezpečnosti. Mnohé výzvy majú špecifickú alokáciu pre MSP.

Národné podporné nástroje na Slovensku

Na národnej úrovni sú dostupné ďalšie nástroje podpory. Slovak Business Agency poskytuje poradenské služby, vzdelávacie programy a informácie o podporných schémach pre MSP vrátane oblasti digitalizácie. Slovenská inovačná a energetická agentúra (SIEA) administruje programy podpory inovácií a digitalizácie financované z európskych a národných zdrojov.

Významným zdrojom podpory sú zároveň aj prostriedky poskytované v rámci **operačných programov financovaných z európskych štrukturálnych a investičných fondov (EŠIF)**, resp. v súčasnom programovom období najmä z fondov politiky súdržnosti EÚ. Tieto programy môžu predstavovať dôležitý finančný rámec pre podporu digitalizácie, inovácií, rozvoja kybernetickej bezpečnosti, výskumu a vývoja, ako aj pre posilňovanie technologickej pripravenosti malých a stredných podnikov. Pre MSP preto môžu byť operačné programy významným nástrojom na zmiernenie nákladov spojených s adaptáciou na nové technologické regulácie.

Národný bezpečnostný úrad (NBÚ) je kompetentným orgánom pre kybernetickú bezpečnosť na Slovensku a poskytuje usmernenia k implementácii NIS2 a súvisiacich predpisov. Úrad pre reguláciu elektronických komunikácií a poštových služieb môže zohrávať úlohu pri implementácii určitých aspektov digitálnych regulácií.

Odborové a sektorové združenia

Odborové a sektorové združenia môžu poskytovať špecializovanú podporu a facilitovať zdieľanie skúseností medzi MSP. IT Asociácia Slovenska združuje podniky v IT sektore a môže poskytovať informácie o reguláciách relevantných pre IT priemysel. Slovenská obchodná a priemyselná komora poskytuje všeobecnú podporu pre podnikateľov vrátane informácií o regulačných zmenách. Sektorové asociácie v oblastiach ako finančné služby, zdravotníctvo alebo energetika môžu poskytovať špecifické usmernenia pre svoje členské organizácie.

Komerčné nástroje a služby

Na trhu sú dostupné komerčné nástroje a služby, ktoré môžu uľahčiť compliance. Softvérové nástroje zahŕňajú platformy pre GRC (Governance, Risk, Compliance), nástroje pre správu SBOM, SIEM systémy a nástroje pre monitoring zraniteľností. Konzultačné služby od špecializovaných konzultačných spoločností poskytujú poradenstvo pri implementácii regulačných požiadaviek.

Certifikačné orgány sú akreditované organizácie poskytujúce certifikáciu podľa štandardov ako ISO 27001. Managed security services (MSSP) sú poskytovatelia bezpečnostných služieb, ktorí môžu prevziať časť bezpečnostných funkcií na outsourcing.

Tab. č. 20: **Prehľad zdrojov podpory pre MSP**

Typ zdroja	Príklady	Typ podpory
EÚ nástroje	EDIH, sandboxy, TEFs, granty	Testovanie, školenia, poradenstvo, financovanie
Národné inštitúcie	SBA, SIEA, NBÚ	Poradenstvo, financovanie, usmernenia
Združenia	ITAS, SOPK, sektorové asociácie	Networking, zdieľanie skúseností, advocacy
Komerčné služby	Konzultanti, SW nástroje, MSSP	Implementácia, automatizácia, outsourcing
Certifikačné orgány	Akreditované certifikačné orgány	Formálna certifikácia (ISO 27001 a pod.)

Zdroj: Vlastné spracovanie

4.5.5 Scenáre vývoja a dlhodobá perspektíva

Pre strategické plánovanie je užitočné zvážiť možné scenáre vývoja regulačného prostredia a trhu v strednodobom až dlhodobom horizonte. Hoci predikcia budúcnosti je neistá, identifikácia pravdepodobných trendov môže pomôcť MSP pripraviť sa na rôzne eventuality.

Scenár 1: Rozširovanie regulačného rozsahu

Prvý scenár predpokladá pokračujúce rozširovanie regulačného rozsahu na ďalšie sektory, technológie a veľkostné kategórie podnikov. V tomto scenári sa MSP, ktoré dnes nie sú priamo regulované, postupne stanú subjektmi regulácie. Prahy pre zaradenie medzi regulované subjekty (napríklad veľkostné kritériá NIS2) sa môžu znižovať.

Pre MSP je implikáciou tohto scenára, že aj tie, ktoré dnes zvolia minimalistický prístup, budú musieť v budúcnosti investovať do compliance. Proaktívny prístup dnes môže byť nákladovo efektívnejší ako reaktívna adaptácia v budúcnosti pod časovým tlakom.

Scenár 2: Globálna konvergencia

Druhý scenár predpokladá, že Bruselský efekt povedie k širokej globálnej konvergencii regulačných prístupov. Tretie krajiny prijmú regulácie podobné AI Act, CRA a NIS2, čím sa európske štandardy stanú de facto globálnymi štandardmi.

Pre MSP je implikáciou, že investície do súladu s reguláciami EÚ budú mať hodnotu aj pri expanzii na tretie trhy. MSP budujúce compliance kapacity dnes si vytvárajú základ pre globálnu konkurencieschopnosť.

Scenár 3: Technologická akcelerácia

Tretí scenár predpokladá, že tempo technologického vývoja, najmä v oblasti AI, predstihne schopnosť regulátorov reagovať. Nové technológie a aplikácie budú vznikať rýchlejšie, než budú môcť byť regulované, čo vytvorí obdobia regulačnej neistoty.

Pre MSP je implikáciou potreba flexibility a schopnosti rýchlo sa adaptovať. MSP by mali budovať interné kapacity pre hodnotenie regulačných implikácií nových technológií a byť pripravené na rýchle zmeny požiadaviek.

Scenár 4: Regulačné zjednodušenie

Štvrtý scenár predpokladá, že pod tlakom na konkurencieschopnosť Európy dôjde k zjednodušeniu regulačného rámca, väčšej diferenciácii požiadaviek pre MSP a rozšíreniu výnimiek. Tento scenár je menej pravdepodobný v krátkodobom horizonte, ale môže sa realizovať v strednodobom období, ak sa prejaví negatívny dopad regulácií na inovácie.

Pre MSP je implikáciou, že investície do compliance by mali byť škálovateľné a flexibilné, aby bolo možné ich znížiť v prípade zjednodušenia požiadaviek. Súčasne by MSP mali sledovať politickú diskusiu a aktívne sa zapájať do konzultačných procesov.

4.5.6 Zhrnutie a kľúčové závery

Kapitola 4 analyzovala nepriame dopady technologických regulácií EÚ na slovenské MSP naprieč štyrmi kľúčovými dimenziami: vplyv na inovačný potenciál, prístup na trhy, reputačné efekty a dodávateľské reťazce. Analýza ukázala, že tieto nepriame dopady sú často rovnako významné ako priame náklady compliance a môžu rozhodnúť o dlhodobej konkurencieschopnosti MSP.

Syntéza kľúčových zistení

V oblasti inovácií regulácie vytvárajú duálny efekt. Poskytujú podporné nástroje (sandboxy, EDIH, TEFs), ale súčasne odčerpávajú zdroje z výskumu a vývoja. Empirické dôkazy z GDPR naznačujú, že menšie podniky sú zasiahnuté proporcionálne viac, čo vytvára riziko koncentrácie trhu.

V oblasti trhov harmonizácia prináša významné prínosy v podobe jednotného regulačného rámca pre 450 miliónov spotrebiteľov. Súčasne vznikajú nové trhové príležitosti v oblasti compliance služieb a technológií. Bruselský efekt rozširuje relevanciu compliance podľa EÚ na globálnej úrovni.

V oblasti reputácie sa kybernetická bezpečnosť a etický prístup k AI stávajú konkurenčnými diferenciátormi. Empirické dáta ukazujú, že značná časť organizácií už dnes vyžaduje bezpečnostnú certifikáciu od dodávateľov a tento trend sa bude zosilňovať.

V oblasti dodávateľských reťazcov kaskádová zodpovednosť a požiadavky na bezpečnosť tretích strán vytvárajú nové povinnosti pre MSP vo všetkých pozíciách. Dramatický nárast útokov na supply chain od roku 2020 podčiarkuje reálnosť týchto rizík.

Kľúčové odporúčania pre slovenské MSP

Na základe analýzy formulujeme päť kľúčových strategických odporúčaní pre slovenské MSP.

- Po prvé, vykonať strategickú analýzu a zvoliť explicitnú pozíciu. Každé MSP by malo vyhodnotiť svoju regulačnú expozíciu, dostupné zdroje a strategické ambície a na základe tejto analýzy zvoliť jednu zo strategických pozícií (líder, rýchly nasledovník, minimalistický adaptér alebo strategický exiter).

- Po druhé, maximálne využiť dostupnú podpornú infraštruktúru. EÚ a národné inštitúcie poskytujú rozsiahlu podporu, ktorej nevyužitie znamená zbytočnú konkurenčnú nevýhodu. EDIH, sandboxy, granty a poradenské služby môžu významne znížiť náklady compliance.

- Po tretie, integrovať compliance do podnikovej stratégie. Compliance by nemalo byť izolovaným projektom, ale integrálnou súčasťou produktovej stratégie, HR stratégie a vzťahov so zákazníkmi. Bezpečnosť a etika by sa mali stať súčasťou hodnoty, ktorú MSP poskytuje zákazníkom.

- Po štvrté, budovať interné kapacity. Dlhodobá konkurencieschopnosť vyžaduje interné kompetencie v oblasti bezpečnosti, AI a compliance. Investície do vzdelávania zamestnancov a prípadne špecializovaných pozícií sa vrátia v podobe nižšej závislosti na externých zdrojoch a lepšej pripravenosti na budúce zmeny.

- Po piate, sledovať vývoj a byť pripravený na adaptáciu. Regulačné prostredie sa bude ďalej vyvíjať. MSP by mali systematicky monitorovať regulačný vývoj, participovať na konzultačných procesoch a byť pripravené na úpravu svojej stratégie v reakcii na zmeny.

Technologické regulácie EÚ predstavujú pre slovenské MSP fundamentálnu zmenu podnikateľského prostredia. MSP, ktoré túto zmenu pochopia, prijmú a strategicky na ňu zareagujú, môžu z nej vyjsť posilnené. Tie, ktoré ju budú ignorovať alebo vnímať len ako záťaž, riskujú dlhodobú stratu konkurencieschopnosti. Voľba je na samotných podnikoch.

Okrem priamych nákladov na zabezpečenie súladu s reguláciami AI Act, CRA a NIS2, ktoré boli analyzované v predchádzajúcej kapitole, čelia malé a stredné podniky aj významným nepriamym dopadom. Tieto nepriame efekty sa prejavujú v oblastiach inovačného potenciálu, prístupu na trhy, reputačných vplyvov a postavenia v dodávateľských reťazcoch. Nepriame dopady môžu byť pre mnohé MSP rovnako významné, prípadne aj závažnejšie ako priame náklady, pretože ovplyvňujú strategické rozhodovanie, konkurenčnú pozíciu a dlhodobú udržateľnosť podnikania.

Táto kapitola skúma komplexný obraz nepriamych dopadov regulácií a identifikuje príležitosti, ktoré môžu MSP využiť, ako aj riziká, ktorým musia čeliť. Analýza vychádza z dostupných štúdií, odborných publikácií a skúseností z implementácie obdobných regulačných rámcov. Zohľadňuje tiež špecifiká slovenských MSP, ktoré často disponujú limitovanými finančnými a personálnymi kapacitami a majú obmedzený prístup k špecializovanému právnemu a technologickému poradenstvu.

5 PRÁVNY RÁMEC A INŠTITUCIONÁLNA INFRAŠTRUKTÚRA NA SLOVENSKU

Implementácia technologických regulácií Európskej únie v podmienkach Slovenskej republiky vyžaduje komplexnú analýzu právneho rámca, inštitucionálnej infraštruktúry a špecifických aspektov transpozície. Táto kapitola sa zameriava na podrobnú analýzu transpozície smernice NIS2, nariadenia AI Act a nariadenia CRA do slovenského právneho poriadku, identifikáciu prípadného goldplatingu, mapovanie dozorných orgánov a ich kompetencií, ako aj na analýzu sankčného režimu.

Pre malé a stredné podniky je pochopenie právneho rámca kľúčové pre správne nastavenie compliance stratégie a efektívnu alokáciu zdrojov. Kapitola poskytuje praktický prehľad, ktorý MSP umožní orientovať sa v regulačnom prostredí a identifikovať relevantné povinnosti.

5.1 Analýza transpozície do slovenského právneho poriadku

Transpozícia európskych smerníc a implementácia nariadení do národného právneho poriadku predstavuje komplexný proces, ktorý ovplyvňuje rozsah a spôsob uplatňovania regulácií na národnej úrovni. V prípade Slovenskej republiky je tento proces determinovaný ústavným rámcom, legislatívnymi pravidlami vlády a metodickými usmerneniami pre posudzovanie vplyvov.

5.1.1 Transpozícia smernice NIS2

Smernica NIS2 (Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555) bola do slovenského právneho poriadku transponovaná prostredníctvom novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. Novela bola schválená Národnou radou Slovenskej republiky dňa 28. novembra 2024 a vyhlásená v Zbierke zákonov ako zákon č. 366/2024 Z. z. s účinnosťou od 1. januára 2025.

Kľúčové zmeny oproti predchádzajúcej právnej úprave

Novela zákona o kybernetickej bezpečnosti prináša niekoľko zásadných zmien. Rozširuje sa okruh regulovaných subjektov, pričom sa mení mechanizmus ich identifikácie. Kým predchádzajúca právna úprava vychádzala z kombinovaného spôsobu určenia podľa prílohy zákona, nová úprava zavádza prahovú hodnotu veľkosti subjektu v súlade s odporúčaním Komisie 2003/361/ES. Regulácia sa tak vzťahuje na stredné podniky (50 až 249 zamestnancov, ročný obrat 10 až 50 miliónov EUR) a väčšie subjekty v definovaných sektoroch.

Ďalšou významnou zmenou je zrušenie kategorizácie a klasifikácie informácií a informačných systémov, ktorú nahrádza analýza rizík ako univerzálny nástroj pre aplikáciu bezpečnostných opatrení. Posilňuje sa tiež úprava bezpečnosti dodávateľského reťazca a hlásenia kybernetických bezpečnostných incidentov.

Rozsah pôsobnosti

Zákon sa vzťahuje na prevádzkovateľov základných služieb, ktorí sa delia na dve kategórie. Kľúčové subjekty vykonávajú kritickú základnú službu a patria sem subjekty prekračujúce limity stredného podniku v najdôležitejších sektoroch ako energetika, doprava, bankovníctvo, infraštruktúra finančného trhu, zdravotníctvo, pitná a odpadová voda, digitálna infraštruktúra, správa IKT služieb B2B, verejná správa a vesmír. Dôležité subjekty zahŕňajú ostatných prevádzkovateľov základných služieb, ktorí spĺňajú veľkostné kritériá v regulovaných sektoroch.

Podľa dôvodovej správy k zákonu sa novela dotýka na Slovensku najmenej 3 403 organizácií. Tento počet predstavuje významné rozšírenie oproti predchádzajúcej právnej úprave.

Tab. č. 21: **Porovnanie právnej úpravy NIS1 a NIS2 na Slovensku**

Aspekt	NIS1 (do 31.12.2024)	NIS2 (od 1.1.2025)
Počet sektorov	7 sektorov	18 sektorov
Identifikácia subjektov	Kombinovaný spôsob	Veľkostné kritériá
Odhadovaný počet subjektov	cca 1 500	min. 3 403
Maximálna sankcia	300 000 EUR	10 mil. EUR / 2 % obratu
Prístup k rizikám	Kategorizácia IS	Analýza rizík

Zdroj: Zákon č. 69/2018 Z. z. v znení účinnom do 31.12.2024 a od 1.1.2025

5.1.2 Implementácia AI Act

Nariadenie o umelej inteligencii (AI Act, nariadenie 2024/1689) je nariadením s priamou aplikáciou, čo znamená, že nevyžaduje transpozíciu v klasickom zmysle. Napriek tomu si vyžaduje prijatie národnej legislatívy v niekoľkých oblastiach, najmä určenie dozorných orgánov, stanovenie pravidiel pre regulačné sandboxy a úpravu sankčného režimu.

Stav prípravy národnej legislatívy

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (MIRRI) predložilo v auguste 2025 do medzirezortného pripomienkového konania návrh zákona o umelej inteligencii. Cieľom zákona je zabezpečiť uplatňovanie kľúčových ustanovení AI Act a vytvoriť rámec pre inštitucionálne usporiadanie a výkon dohľadu nad systémami AI na Slovensku.

Podľa návrhu bude MIRRI pôsobiť ako centrálny orgán dohľadu nad AI na Slovensku. Okrem monitorovania systémov umelej inteligencie bude koordinovať činnosti ostatných príslušných orgánov a zabezpečovať jednotný postup pri dohľade nad využívaním AI. Slovensko má ambíciu zaradiť sa medzi krajiny, ktoré budú mať vlastný vykonávací zákon v účinnosti medzi prvými v EÚ.

Časový harmonogram účinnosti AI Act

Nariadenie nadobúda účinnosť postupne. Od 2. februára 2025 platia ustanovenia o zakázaných praktikách AI a požiadavky na gramotnosť v oblasti AI. Od 2. augusta 2025 platia pravidlá pre modely AI na všeobecné účely a členské štáty musia zriadiť oznamujúce orgány. Plná účinnosť nariadenia vrátane pravidiel pre vysokorizikové AI systémy nastáva od 2. augusta 2026. Od 2. augusta 2027 budú účinné pravidlá pre vysokorizikové AI systémy zabudované do regulovaných výrobkov.

Tab. č. 22: **Časový harmonogram účinnosti AI Act**

Dátum	Účinné ustanovenia
2.2.2025	Zakázané praktiky AI, požiadavky na gramotnosť
2.8.2025	Modely AI na všeobecné účely, oznamujúce orgány
2.8.2026	Plná účinnosť vrátane vysokorizikových AI systémov
2.8.2027	Vysokorizikové AI v regulovaných výrobkoch

Zdroj: Nariadenie 2024/1689, článok 113

5.1.3 Implementácia CRA

Cyber Resilience Act (CRA, nariadenie 2024/2847) je taktiež nariadením s priamou aplikáciou. Nariadenie nadobudlo platnosť 10. decembra 2024 a hlavné povinnosti sa začnú uplatňovať od 11. decembra 2027, čo poskytuje výrobcom 36-mesačné prechodné obdobie na prispôsobenie sa novým požiadavkám.

Požiadavky na národnú implementáciu

CRA vyžaduje od členských štátov prijatie niekoľkých opatrení. Je potrebné určiť orgány dozoru nad trhom, ktoré budú zodpovedné za kontrolu súladnosti produktov s digitálnymi prvkami. Ďalej je potrebné určiť notifikačné orgány pre posudzovanie zhody a stanoviť pravidlá pre ukladanie sankcií.

Na Slovensku zatiaľ nebolo prijaté formálne rozhodnutie o určení týchto orgánov. Predpokladá sa, že úlohu orgánu dozoru nad trhom bude plniť Národný bezpečnostný úrad v spolupráci so Slovenskou obchodnou inšpekciou. Notifikačným orgánom by mala byť Slovenská národná akreditačná služba.

Skrátené lehoty pre hlásenie

Dôležitým aspektom CRA sú skrátené lehoty pre niektoré povinnosti. Požiadavky na hlásenie zraniteľností a incidentov sa začnú uplatňovať už 21 mesiacov po nadobudnutí platnosti nariadenia, teda od septembra 2026. Výrobcovia produktov s digitálnymi prvkami tak budú musieť zaviesť procesy pre hlásenie skôr, ako nadobudnú účinnosť všetky ostatné povinnosti.

Tab. č. 23: **Časový harmonogram implementácie CRA**

Dátum	Míľnik
10.12.2024	Nadobudnutie platnosti nariadenia
9/2026	Účinnosť požiadaviek na hlásenie (21 mesiacov)
11.12.2027	Plná účinnosť všetkých povinností (36 mesiacov)

Zdroj: Nariadenie CRA, článok 71

5.1.4 Vzájomné vzťahy medzi reguláciami

Technologické regulácie EÚ tvoria vzájomne prepojenú sieť, v ktorej sa jednotlivé predpisy dopĺňajú a na seba nadväzujú. Pre MSP je dôležité chápať tieto vzťahy, aby mohli efektívne plánovať compliance aktivity.

Vzťah NIS2 a CRA

Smernica NIS2 a nariadenie CRA sú komplementárne. Zatiaľ čo NIS2 reguluje prevádzkovateľov služieb a zameriava sa na ich procesy a systémy riadenia kybernetickej bezpečnosti, CRA reguluje výrobcov produktov a zameriava sa na bezpečnosť samotných produktov. Subjekt, ktorý je prevádzkovateľom základnej služby podľa NIS2 a zároveň používa produkty s digitálnymi prvkami, musí plniť požiadavky oboch regulácií.

Vzťah AI Act a CRA

AI Act a CRA sa môžu prekrývať v prípade AI systémov, ktoré sú súčasťou produktov s digitálnymi prvkami. V takom prípade platí, že produkt musí spĺňať požiadavky oboch nariadení. AI Act výslovne stanovuje, že splnenie požiadaviek CRA na kybernetickú bezpečnosť sa považuje za splnenie príslušných požiadaviek AI Act.

Tab. č. 24: **Vzájomné vzťahy medzi technologickými reguláciami**

Regulácia	Primárny fokus	Vzťah k ostatným
NIS2	Prevádzkovatelia služieb	Komplementárna s CRA
AI Act	AI systémy	Nadväzuje na CRA, GDPR
CRA	Produkty s digit. prvkami	Dopĺňa NIS2, AI Act

Zdroj: Vlastné spracovanie na základe textov regulácií

5.2 Identifikácia prípadného goldplatingu

Goldplating predstavuje prax, pri ktorej členské štáty pri transpozícii smerníc EÚ stanovujú dodatočné požiadavky nad rámec toho, čo európska legislatíva priamo vyžaduje. Tento fenomén môže mať významné dopady na konkurencieschopnosť podnikov, pretože vytvára prísnejšie podmienky pre subjekty pôsobiace v danom členskom štáte v porovnaní s ich konkurentmi v iných krajinách EÚ.

Táto podkapitola analyzuje, či a v akom rozsahu došlo pri transpozícii technologických regulácií, najmä smernice NIS2, ku goldplatingu v podmienkach Slovenskej republiky.

5.2.1 Metodologický rámec pre identifikáciu goldplatingu na Slovensku

Slovenská republika zaviedla v roku 2022 systematický rámec pre identifikáciu a prevenciu neopodstatneného goldplatingu. Tento rámec je súčasťou reformy v rámci Komponentu č. 14 Plánu obnovy a odolnosti SR.

Zavedenie ochrany pred neopodstatneným goldplatingom

Reforma bola zavedená prostredníctvom novely Jednotnej metodiky na posudzovanie vybraných vplyvov, schválenej uznesením vlády SR č. 383/2022 dňa 8. júna 2022. Uplatňovanie reformy je zabezpečované s účinnosťou od 31. decembra 2022 prostredníctvom Jednotnej metodiky a Legislatívnych pravidiel vlády Slovenskej republiky.

Cieľom reformy je zabrániť neprimeranému rozširovaniu obsahu národných právnych predpisov nad rámec minimálnych požiadaviek legislatívy EÚ. Ministerstvo hospodárstva SR je gestorom lepšej regulácie a zodpovedným orgánom za koordináciu tejto agendy.

Formy goldplatingu

Podľa definície v Jednotnej metodike môže goldplating nadobúdať rôzne podoby. Prvou formou je rozšírenie pôsobnosti smernice na ďalšie subjekty, na ktoré sa primárne povinnosť nevzťahovala. Druhou formou je sprísnenie požiadaviek nad úroveň stanovenú smernicou. Treťou formou je nevyužitie výnimiek, ktoré smernica umožňuje. Štvrtou formou je predčasná transpozícia, keď účinnosť nastane skôr ako posledný možný termín stanovený smernicou. Piatou formou sú takzvané skryté novely alebo prílepky, teda využitie procesu transpozície na zavedenie vnútroštátnej právnej úpravy, ktorá nepatrí pod účel a cieľ smernice.

Tab. č. 25: **Kategórie goldplatingu a ich charakteristiky**

Kategória goldplatingu	Popis	Dopad na MSP
Rozšírenie pôsobnosti	Zahrnutie ďalších subjektov	Regulácia aj MSP mimo rozsahu
Sprísnenie požiadaviek	Vyššia úroveň povinností	Vyššie náklady na compliance
Nevyužitie výnimiek	Neuplatnenie flexibility	Zbytočná záťaž
Predčasná transpozícia	Skoršia účinnosť	Kratší čas na prípravu
Skryté novely	Nesúvisiace ustanovenia	Nepredvídateľná záťaž

Zdroj: Jednotná metodika na posudzovanie vybraných vplyvov, MH SR

5.2.2 Analýza transpozície NIS2 z hľadiska goldplatingu

Pri analýze transpozície smernice NIS2 do slovenského právneho poriadku prostredníctvom novely zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti je potrebné skúmať jednotlivé oblasti, kde mohlo dôjsť ku goldplatingu.

Rozsah pôsobnosti – regulované subjekty

Smernica NIS2 stanovuje veľkostné kritériá pre určenie regulovaných subjektov. Podľa článku 2 sa smernica vzťahuje na subjekty, ktoré sú stredným podnikom podľa

odporúčania Komisie 2003/361/ES (50 až 249 zamestnancov, ročný obrat 10 až 50 miliónov EUR) alebo ho presahujú.

Slovenská transpozícia v § 17 novely zákona o kybernetickej bezpečnosti v zásade kopíruje tieto veľkostné kritériá. Zároveň však zahŕňa niektoré kategórie subjektov bez ohľadu na ich veľkosť, napríklad poskytovateľov dôveryhodnej služby, správcov TLD domén, poskytovateľov verejnej elektronickej komunikačnej siete a subjekty, ktorých narušenie by mohlo mať významný vplyv na verejný poriadok, bezpečnosť alebo verejné zdravie. Toto rozšírenie však nie je goldplatingom, pretože vychádza priamo z ustanovení NIS2.

Sankcie a pokuty

Oblasť sankcií je často citlivou z hľadiska goldplatingu. Smernica NIS2 v článku 34 stanovuje maximálne výšky sankcií: pre základné subjekty minimálne 10 miliónov EUR alebo 2 % celkového celosvetového ročného obratu, pre dôležité subjekty minimálne 7 miliónov EUR alebo 1,4 % obratu.

Slovenská transpozícia v § 31 novely stanovuje sankcie v nasledujúcom rozsahu: pokuty od 300 do 500 000 EUR za administratívne porušenia, pokuty do 7 000 000 EUR alebo 1,4 % obratu za závažnejšie porušenia a maximálne pokuty do 10 000 000 EUR alebo 2 % obratu pre najzávažnejšie porušenia. Porovnanie ukazuje, že slovenská úprava sa drží v medziach stanovených smernicou a neprekračuje maximálne výšky sankcií.

Tab. č. 26: **Porovnanie sankcií – NIS2 vs. slovenská transpozícia**

Typ subjektu / porušenia	NIS2 (minimum)	SR transpozícia
Základné subjekty – max.	10 mil. EUR / 2 % obratu	10 mil. EUR / 2 % obratu
Dôležité subjekty – max.	7 mil. EUR / 1,4 % obratu	7 mil. EUR / 1,4 % obratu
Administratívne porušenia	Nestanovené	300 – 500 000 EUR
Individuálna zodpovednosť	Umožnená	Do 5 000 EUR

Zdroj: Smernica NIS2, zákon č. 366/2024 Z. z.

Dodávateľský reťazec

Oblasť bezpečnosti dodávateľského reťazca je v slovenskej transpozícii upravená podrobnejšie než v samotnej smernici. Novela zákona stanovuje povinnosť uzavrieť písomnú zmluvu o zabezpečení plnenia bezpečnostných opatrení a povinnosť dodávateľa podrobiť sa kontrole. U dodávateľov so zmluvou s prevádzkovateľom kritickej základnej služby môže kontrolu vykonávať priamo NBÚ.

Toto rozšírenie možno kvalifikovať ako opodstatnený goldplating odôvodnený špecifikami slovenského trhu a potrebou efektívnej kontroly. Účely sú legitímne – ochrana kritickej infraštruktúry a zabezpečenie, že bezpečnostné štandardy sú dodržované v celom dodávateľskom reťazci.

5.2.3 Analýza požiadaviek AI Act a CRA

AI Act a CRA sú nariadeniami s priamou aplikáciou, čo znamená, že v zásade nevytvárajú priestor pre goldplating v klasickom zmysle – členské štáty nemajú možnosť meniť ich ustanovenia pri transpozícii. Napriek tomu existujú oblasti, kde národná implementácia môže zaviesť dodatočné požiadavky.

AI Act poskytuje členským štátom diskreciu v niekoľkých oblastiach: určenie dozorných orgánov, pravidlá pre regulačné sandboxy a detaily sankčného režimu. Slovensko sa rozhodlo pre MIRRI ako centrálny orgán, čo je legitímna voľba v rámci flexibility nariadenia.

CRA ako nariadenie tiež nevyžaduje transpozíciu, ale členské štáty musia určiť orgány dozoru nad trhom a notifikované orgány. Zatiaľ nie sú známe zámery zavádzať dodatočné požiadavky nad rámec nariadenia.

Tab. č. 27: **Porovnanie prístupov k transpozícii NIS2 vo vybraných štátoch**

Aspekt	Slovensko	Maďarsko	Česko (návrh)
Veľkostné kritériá	Podľa smernice	Podľa smernice	Podľa smernice
Rozšírenie pôsobnosti	Limitované	Minimálne	Minimálne
Maximálne sankcie	Podľa smernice	Podľa smernice	Podľa smernice
Dodávateľský reťazec	Podrobnejšie	Základné	Základné

Zdroj: Vlastný výskum na základe národných transpozícií

5.2.4 Celkové hodnotenie a dopady na MSP

Na základe vykonanej analýzy možno konštatovať, že slovenská transpozícia technologických regulácií EÚ nevykazuje významný neopodstatnený goldplating. Slovensko v zásade postupovalo v súlade s metodologickým rámcom pre identifikáciu goldplatingu a držalo sa minimálnych požiadaviek smerníc.

Jedinou výraznejšou oblasťou, kde možno identifikovať prvky goldplatingu, je úprava bezpečnosti dodávateľského reťazca. Tento goldplating však možno kvalifikovať ako opodstatnený z dôvodov ochrany kritickej infraštruktúry.

Pre malé a stredné podniky znamená absencia významného goldplatingu, že ich záťaž je porovnateľná so záťažou MSP v iných členských štátoch. MSP na Slovensku nie sú vystavené konkurenčnej nevýhode voči MSP v iných krajinách EÚ v dôsledku prísnejšej národnej regulácie.

5.3 Identifikácia dozorných orgánov a ich kompetencie

Efektívna implementácia technologických regulácií EÚ vyžaduje funkčnú inštitucionálnu infraštruktúru na národnej úrovni. Každá z analyzovaných regulácií – NIS2, AI Act a CRA – vyžaduje určenie príslušných orgánov zodpovedných za dozor, presadzovanie a spoluprácu s európskymi inštitúciami.

Pre malé a stredné podniky je znalosť príslušných orgánov kritická – umožňuje im vedieť, kam sa obrátiť v prípade otázok, kde hľadať usmernenia a s akými kontrolnými orgánmi môžu prísť do kontaktu.

5.3.1 Národný bezpečnostný úrad – kľúčový orgán pre kybernetickú bezpečnosť

Národný bezpečnostný úrad (NBÚ) je ústredný orgán štátnej správy Slovenskej republiky s kľúčovou úlohou v oblasti kybernetickej bezpečnosti. Jeho kompetencie pokrývajú najmä implementáciu smernice NIS2 a čiastočne aj CRA.

Právne zakotvenie a všeobecné kompetencie

NBÚ je ústredným orgánom štátnej správy pre ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby. Kontrolu činnosti úradu vykonáva Národná rada Slovenskej republiky. Na čele úradu stojí riaditeľ, ktorý zodpovedá za jeho činnosť, riadi a reprezentuje úrad navonok.

V oblasti kybernetickej bezpečnosti je NBÚ národnou autoritou pre kybernetickú bezpečnosť. Riadi a koordinuje výkon štátnej správy v oblasti kybernetickej bezpečnosti, určuje štandardy a vydáva politiku správania sa v kybernetickom priestore. Úrad je hlavným kontaktným bodom pre zahraničie v oblasti kybernetickej bezpečnosti.

Kompetencie podľa zákona o kybernetickej bezpečnosti

Podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení novely č. 366/2024 Z. z. má NBÚ nasledujúce hlavné kompetencie: vedie register prevádzkovateľov základných služieb a rozhoduje o zápise subjektov do tohto registra, vykonáva dozor nad dodržiavaním povinností regulovaných subjektov, prijíma hlásenia o kybernetických bezpečnostných incidentoch a koordinuje reakciu na ne, vydáva právne predpisy v oblasti bezpečnostných opatrení.

V rámci NBÚ funguje Národná jednotka pre riešenie kybernetických bezpečnostných incidentov SK-CERT. Táto jednotka plní úlohy Computer Security Incident Response Team (CSIRT) na národnej úrovni.

Tab. č. 28: **Hlavné kompetencie NBÚ v oblasti technologických regulácií**

Oblasť	Kompetencia	Právny základ
NIS2 – regulácia	Vedie register, dozor, sankcie	Zákon č. 69/2018 Z. z.
NIS2 – incidenty	Prijíma hlásenia, koordinuje	SK-CERT
NIS2 – medzinárodné	Jednotné kontaktné miesto	Čl. 8 NIS2
CRA – dozor	Orgán dozoru (predpoklad)	CRA čl. 52

Zdroj: Zákon o kybernetickej bezpečnosti, webová stránka NBÚ

5.3.2 Ministerstvo investícií, regionálneho rozvoja a informatizácie SR

MIRRI je kľúčovým orgánom pre implementáciu AI Act na Slovensku. Jeho kompetencie v oblasti umelej inteligencie sa postupne rozširujú v súlade s požiadavkami európskej legislatívy.

Podľa návrhu národnej legislatívy predloženej v roku 2025 bude MIRRI pôsobiť ako centrálny orgán dohľadu nad AI na Slovensku. Okrem monitorovania systémov umelej inteligencie bude koordinovať činnosti ostatných príslušných orgánov a zabezpečovať jednotný postup pri dohľade.

V rámci MIRRI pôsobí Splnomocnenec vlády SR pre umelú inteligenciu, ktorým je štátny tajomník Radoslav Štefánek. Splnomocnenec koordinuje aktivity súvisiace s AI na národnej úrovni a zastupuje Slovensko v medzinárodných fórach.

Dňa 2. novembra 2020 bola zriadená Stála komisia pre etiku a reguláciu umelej inteligencie (CERAI). Je to nezávislý odborný a poradný orgán zriadený MIRRI, ktorého úlohou je posudzovanie etických, sociálno-spoločenských a právnych otázok súvisiacich s AI.

5.3.3 Slovenská obchodná inšpekcia

Slovenská obchodná inšpekcia (SOI) je orgánom štátnej kontroly vnútorného trhu vo veciach ochrany spotrebiteľa s celoslovenskou pôsobnosťou. V kontexte technologických regulácií bude mať SOI významnú úlohu pri dozore nad trhom podľa CRA.

SOI je podriadená Ministerstvu hospodárstva SR a vykonáva dozor nad viac ako 350 predpismi. Jej hlavné kompetencie zahŕňajú kontrolu predaja výrobkov a poskytovania služieb spotrebiteľom, štátny dozor v energetike a dohľad nad trhom podľa osobitných predpisov.

V oblasti trhového dozoru SOI vykonáva kontrolu zhody výrobkov s technickými požiadavkami vrátane overovania označenia CE. Tieto kompetencie sú priamo relevantné pre implementáciu CRA.

5.3.4 Ďalšie relevantné orgány

Okrem hlavných dozorných orgánov existuje niekoľko ďalších inštitúcií s relevantnými kompetenciami. Úrad na ochranu osobných údajov SR (ÚOOÚ) je nezávislým orgánom dozoru nad spracúvaním osobných údajov podľa GDPR. V kontexte AI Act má ÚOOÚ relevanciu, pretože mnohé AI systémy spracúvajú osobné údaje.

Pre vysokorizikové AI systémy v konkrétnych sektoroch môžu mať kompetencie sektorové regulačné orgány, napríklad Národná banka Slovenska pre AI systémy vo finančnom sektore, Štátny ústav pre kontrolu liečiv pre AI v zdravotníctve alebo Dopravný úrad pre AI v doprave.

Tab. č. 29: **Prehľad dozorných orgánov pre technologické regulácie**

Orgán	NIS2	AI Act	CRA
NBÚ	Hlavný orgán	Spolupráca	Dozor (predpoklad)
MIRRI	–	Centrálny orgán	–
SOI	–	–	Dozor (predpoklad)
ÚOOÚ	–	Spolupráca (GDPR)	–

Zdroj: Vlastné spracovanie na základe platnej a pripravovanej legislatívy

5.3.5 Kapacity dozorných orgánov a výzvy

Efektívny výkon dozorných funkcií vyžaduje adekvátne personálne, technické a finančné kapacity. Analýza súčasného stavu ukazuje niekoľko kľúčových výziev.

Globálny nedostatok odborníkov v oblasti kybernetickej bezpečnosti a umelej inteligencie sa prejavuje aj na Slovensku. Podľa údajov ENISA chýba v Európe viac ako 300 000 odborníkov na kybernetickú bezpečnosť. Dozorné orgány súťažia o týchto odborníkov so súkromným sektorom, ktorý spravidla ponúka vyššie odmeny.

Nové regulácie vytvárajú potrebu koordinácie medzi viacerými orgánmi. Napríklad AI systém využívaný vo finančnom sektore môže spadať pod dozor MIRRI (AI Act), NBS (sektorová regulácia), ÚOOÚ (ochrana osobných údajov) a prípadne NBÚ (kybernetická bezpečnosť). Pre predchádzanie duplicitám je potrebné vytvoriť mechanizmy koordinácie.

5.4 Sankcie

Sankčný režim predstavuje kľúčový nástroj na zabezpečenie dodržiavania regulačných požiadaviek. Technologické regulácie EÚ – NIS2, AI Act a CRA – zavádzajú prísne sankcie za porušenie povinností, pričom výšky pokút môžu dosahovať miliardové sumy pre veľké spoločnosti.

Pre malé a stredné podniky je pochopenie sankčného režimu dôležité pre správne nastavenie rizík a prioritizáciu compliance aktivít.

5.4.1 Sankcie podľa zákona o kybernetickej bezpečnosti (NIS2)

Novela zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, účinná od 1. januára 2025, zavádza diferencovaný sankčný režim v závislosti od typu porušenia a kategórie subjektu.

Štruktúra sankcií

Zákon rozlišuje niekoľko úrovní sankcií podľa závažnosti porušenia. Prvá úroveň pokrýva administratívne porušenia ako neoznámenie začiatku činnosti, neohlásenie zmien, neaktuálnu dokumentáciu alebo neodstránenie nedostatkov z auditu. Za tieto porušenia hrozí pokuta od 300 do 500 000 EUR.

Druhá úroveň sa vzťahuje na závažnejšie porušenia ako neplnenie bezpečnostných opatrení podľa § 20, nehlásenie závažného kybernetického bezpečnostného incidentu podľa

§ 24 alebo nevykonanie nariadení NBÚ. Za tieto porušenia hrozí prevádzkovateľom základnej služby pokuta do 7 000 000 EUR alebo do výšky 1,4 % celkového celosvetového ročného obratu, podľa toho, ktorá suma je vyššia.

Tretia úroveň sa vzťahuje na prevádzkovateľov kritickej základnej služby a zahŕňa najzávažnejšie porušenia. V tomto prípade môže byť uložená pokuta až do 10 000 000 EUR alebo do výšky 2 % celkového celosvetového ročného obratu.

Individuálna zodpovednosť

Novela zákona zavádza aj individuálnu zodpovednosť jednotlivcov. Za nesplnenie niektorých povinností môžu byť zo strany NBÚ sankcionovaní priamo štatutári, zamestnanci alebo manažéri kybernetickej bezpečnosti. Pokuta pre jednotlivcov môže dosiahnuť až 5 000 EUR.

Okrem finančných sankcií môžu byť štatutárom uložené aj ďalšie sankcie vrátane zákazu vykonávať vedúce funkcie. Toto ustanovenie zdôrazňuje osobnú zodpovednosť vedenia za kybernetickú bezpečnosť organizácie.

Tab. č. 30: **Prehľad sankcií podľa zákona o kybernetickej bezpečnosti**

Typ porušenia	Základná služba	Kritická základná služba
Administratívne porušenia	300 – 500 000 EUR	300 – 500 000 EUR
Neplnenie bezp. opatrení	Do 7 mil. EUR / 1,4 % obratu	Do 10 mil. EUR / 2 % obratu
Nehlásenie incidentov	Do 7 mil. EUR / 1,4 % obratu	Do 10 mil. EUR / 2 % obratu
Individuálna zodpovednosť	Do 5 000 EUR	Do 5 000 EUR

Zdroj: Zákon č. 366/2024 Z. z., § 31

5.4.2 Sankcie podľa AI Act

Nariadenie o umelej inteligencii (AI Act) zavádza jeden z najprísnejších sankčných režimov v európskej regulácii. Výška sankcií odráža potenciálnu závažnosť dopadov AI systémov na základné práva a bezpečnosť osôb.

Trojúrovňový systém sankcií

AI Act zavádza trojúrovňový systém sankcií diferencovaný podľa typu porušenia. Najvyššie sankcie sa vzťahujú na zakázané AI praktiky podľa článku 5 nariadenia. Za tieto porušenia hrozí pokuta až do 35 000 000 EUR alebo až do 7 % celkového celosvetového ročného obratu, podľa toho, ktorá suma je vyššia.

Stredná úroveň sankcií sa vzťahuje na porušenie povinností týkajúcich sa vysokorizikových AI systémov. Za tieto porušenia hrozí pokuta až do 15 000 000 EUR alebo až do 3 % celkového celosvetového ročného obratu.

Najnižšia úroveň sankcií sa vzťahuje na ostatné porušenia ako poskytnutie nesprávnych informácií orgánom dohľadu alebo nesplnenie povinnosti transparentnosti. Za tieto porušenia hrozí pokuta až do 7 500 000 EUR alebo až do 1,5 % obratu.

Úľavy pre MSP a startupy

AI Act výslovne zohľadňuje postavenie malých a stredných podnikov a startupov. Pre tieto subjekty sú pokuty nižšie, aby sa zohľadnila ich finančná situácia. Konkrétne, pre MSP a startupy sa uplatňuje nižšia zo dvoch súm – buď fixná suma, alebo percento obratu.

Tab. č. 31: **Prehľad sankcií podľa AI Act**

Typ porušenia	Maximálna pokuta
Zakázané AI praktiky (čl. 5)	35 mil. EUR / 7 % obratu
Vysokorizikové AI systémy	15 mil. EUR / 3 % obratu
Ostatné porušenia	7,5 mil. EUR / 1,5 % obratu

Zdroj: Nariadenie 2024/1689, článok 99

5.4.3 Sankcie podľa CRA

Cyber Resilience Act (CRA) zavádza sankčný režim zameraný na výrobcov produktov s digitálnymi prvkami. Výška sankcií odráža potenciálny dopad nebezpečných produktov na spotrebiteľov a kritickú infraštruktúru.

CRA v článku 64 stanovuje trojúrovňový systém administratívnych pokút. Najvyššie sankcie sa vzťahujú na nedodržanie základných požiadaviek kybernetickej bezpečnosti podľa prílohy I. Za tieto porušenia hrozí pokuta až do 15 000 000 EUR alebo až do 2,5 % celkového celosvetového ročného obratu.

Stredná úroveň sankcií pokrýva porušenia ostatných povinností podľa nariadenia, ako sú povinnosti importérov, distribútorov alebo procesné povinnosti. Za tieto porušenia hrozí pokuta až do 10 000 000 EUR alebo až do 2 % obratu.

Najnižšia úroveň sankcií sa vzťahuje na poskytnutie nesprávnych, neúplných alebo zavádzajúcich informácií notifikovaným orgánom alebo orgánom dozoru nad trhom. Za toto porušenie hrozí pokuta až do 5 000 000 EUR alebo až do 1 % obratu.

CRA výslovne stanovuje, že finančné sankcie sa nevzťahujú na nekomerčný open-source softvér a na tzv. open-source stewardov. Toto ustanovenie má zabezpečiť, aby regulácia neodradila od účasti v open-source komunite.

Tab. č. 32: **Prehľad sankcií podľa CRA**

Typ porušenia	Maximálna pokuta
Základné požiadavky KB (príloha I)	15 mil. EUR / 2,5 % obratu
Ostatné povinnosti	10 mil. EUR / 2 % obratu
Nesprávne/zavádzajúce informácie	5 mil. EUR / 1 % obratu
Open-source steward	Výnimka – bez sankcií

Zdroj: CRA, článok 64

5.4.4 Porovnanie sankcií s inými európskymi predpismi

Pre lepšie pochopenie sankčného režimu technologických regulácií je užitočné porovnať ich s inými významnými európskymi predpismi, najmä GDPR.

Všeobecné nariadenie o ochrane údajov (GDPR) stanovuje maximálne pokuty do 20 000 000 EUR alebo do 4 % celkového celosvetového ročného obratu. V porovnaní s GDPR sú sankcie podľa AI Act vyššie (až 7 % obratu), zatiaľ čo sankcie podľa NIS2 a CRA sú porovnateľné alebo nižšie.

Je však potrebné zdôrazniť, že sankcie podľa rôznych regulácií môžu byť kumulované. Napríklad porušenie pri AI systéme spracúvajúcom osobné údaje môže viesť k sankciám tak podľa AI Act, ako aj podľa GDPR.

Tab. č. 33: **Porovnanie maximálnych sankcií podľa európskych regulácií**

Regulácia	Fixná suma (max.)	% obratu (max.)	Individ. zodp.
GDPR	20 mil. EUR	4 %	Áno
AI Act	35 mil. EUR	7 %	Neurčené
NIS2 (SR)	10 mil. EUR	2 %	Áno (5 000 EUR)
CRA	15 mil. EUR	2,5 %	Neurčené

Zdroj: Vlastné spracovanie na základe textov regulácií

5.4.5 Dopady sankčného režimu na MSP

Pre malé a stredné podniky predstavuje sankčný režim technologických regulácií významné riziko, ale zároveň aj motiváciu pre investície do compliance.

Pre ilustráciu finančného dopadu uvažujme malý podnik s ročným obratom 5 miliónov EUR. V prípade porušenia najzávažnejších ustanovení AI Act by pokuta podľa percentuálneho výpočtu (7 %) činila 350 000 EUR, čo predstavuje 7 % ročného obratu a môže mať existenčné dopady. Pre ten istý podnik by pokuta podľa NIS2 (2 %) činila 100 000 EUR.

Pri ukladaní sankcií sa zohľadňujú poľahčujúce okolnosti. Medzi ne patrí spolupráca s dohliadacím orgánom, dobrovoľné hlásenie porušenia, prijatie nápravných opatrení, predchádzajúca bezúhonnosť subjektu a veľkosť podniku. Pre MSP je preto dôležité komunikovať otvorene s dohľadovými orgánmi a aktívne pracovať na náprave identifikovaných nedostatkov.

5.5 Zhrnutie kapitoly

Piata kapitola analyzovala právny rámec a inštitucionálnu infraštruktúru pre implementáciu technologických regulácií EÚ v podmienkach Slovenskej republiky. Kapitola sa zamerala na tri kľúčové regulácie – smernicu NIS2, nariadenie AI Act a nariadenie CRA – a ich dopady na malé a stredné podniky.

5.5.1 Hlavné zistenia analýzy

Transpozícia a implementácia

Analýza ukázala, že Slovensko pristúpilo k transpozícii a implementácii technologických regulácií zodpovedne a v súlade s požiadavkami EÚ. Novela zákona o kybernetickej bezpečnosti, transponujúca smernicu NIS2, nadobudla účinnosť 1. januára 2025, čo je v rámci termínov stanovených smernicou. Príprava národnej legislatívy pre AI Act prebieha a Slovensko má ambíciu patriť medzi prvé členské štáty s účinným vykonávacím zákonom.

Z hľadiska goldplatingu analýza identifikovala, že slovenská transpozícia v zásade neprekračuje minimálne požiadavky európskej legislatívy. Jedinou výraznejšou oblasťou s prvkami goldplatingu je úprava bezpečnosti dodávateľského reťazca v zákone o kybernetickej bezpečnosti, pričom tento goldplating možno kvalifikovať ako opodstatnený z dôvodov ochrany kritickej infraštruktúry.

Inštitucionálna infraštruktúra

Slovensko má zavedenú funkčnú inštitucionálnu infraštruktúru pre výkon dohľadu nad technologickými reguláciami. NBÚ SR je kľúčovým orgánom pre oblasť kybernetickej bezpečnosti. MIRRI bude centrálnym orgánom dohľadu pre AI Act. SOI bude pravdepodobne zohrávať úlohu pri dozore nad trhom pre CRA.

Sankčný režim

Analýza sankčného režimu ukázala, že technologické regulácie zavádzajú vysoké pokuty, ktoré môžu mať pre MSP existenčné dopady. Maximálne sankcie dosahujú 35 miliónov EUR alebo 7 % obratu (AI Act), 15 miliónov EUR alebo 2,5 % obratu (CRA) a 10 miliónov EUR alebo 2 % obratu (NIS2). Dôležité však je, že regulácie zohľadňujú veľkosť podnikov a pre MSP existujú určité úľavy.

Tab. č. 34: **Súhrn kľúčových parametrov technologických regulácií**

Parameter	NIS2	AI Act	CRA
Typ predpisu	Smernica	Nariadenie	Nariadenie
Účinnosť v SR	1.1.2025	2.8.2025 (postupne)	12/2027 (plná)
Hlavný dozorný orgán	NBÚ	MIRRI	NBÚ/SOI
Max. sankcia	10 mil. / 2 %	35 mil. / 7 %	15 mil. / 2,5 %
Goldplating v SR	Minimálny	N/A (nariadenie)	N/A (nariadenie)

Zdroj: Vlastné spracovanie

5.5.2 Kľúčové výzvy pre MSP

Na základe analýzy možno identifikovať niekoľko kľúčových výziev, ktorým musia MSP čeliť pri implementácii technologických regulácií.

Hlavnou výzvou je komplexnosť a prekrývanie regulácií. MSP môžu súčasne podliehať požiadavkám NIS2, AI Act, CRA, GDPR a sektorovým reguláciám. Orientácia v tomto prostredí vyžaduje značné kapacity, ktoré MSP často nemajú.

Globálny nedostatok odborníkov na kybernetickú bezpečnosť a umelú inteligenciu sa výrazne dotýka MSP, ktoré ťažšie konkurujú veľkým spoločnostiam pri získavaní talentov. Riešením môže byť využívanie externých služieb, zdieľanie odborníkov medzi viacerými MSP alebo investície do vzdelávania existujúcich zamestnancov.

Implementácia regulačných požiadaviek vyžaduje investície do technológií, procesov a ľudí. Pre MSP s obmedzenými zdrojmi môže byť ťažké nájsť potrebné finančné prostriedky. Dôležité je však vnímať tieto investície v kontexte potenciálnych nákladov nesúladnosti – či už vo forme sankcií, alebo v dôsledku kybernetických incidentov.

5.5.3 Odporúčania pre MSP

Na základe vykonanej analýzy možno formulovať nasledujúce odporúčania pre malé a stredné podniky.

Na strategickej úrovni sa odporúča vykonať komplexný audit súčasného stavu a identifikovať, ktoré regulácie sa na podnik vzťahujú. Následne je potrebné vypracovať plán implementácie s jasne definovanými prioritami, termínmi a zodpovednosťami. Dôležité je tiež alokovať adekvátne zdroje a vedenie spoločnosti musí prevziať zodpovednosť za compliance.

Na taktickej úrovni sa odporúča využívať prístup založený na riziku, ktorý umožňuje proporcionálnu implementáciu opatrení. MSP by mali aktívne sledovať usmernenia vydávané dohliadacími orgánmi a využívať konzultačné služby, ktoré orgány poskytujú. Dôležitá je tiež dokumentácia všetkých krokov a rozhodnutí.

Na operatívnej úrovni sa odporúča implementovať základné bezpečnostné opatrenia ako pravidelné aktualizácie, zálohovanie, riadenie prístupov a školenia zamestnancov. Tieto opatrenia sú relevantné pre všetky regulácie a prinášajú okamžité benefity.

Tab. č. 35: **Akčný plán implementácie pre MSP – súhrnné odporúčania**

Fáza	Aktivita	Odporúčaný termín
1. Analýza	Audit súčasného stavu, identifikácia regulácií	Ihneď
2. Plánovanie	Vypracovanie implementačného plánu	Do 1 mesiaca
3. Základné opatrenia	Minimálna KB hygiena, dokumentácia	Do 3 mesiacov
4. Rozšírené opatrenia	Analýza rizík, bezpečnostné politiky	Do 6 mesiacov
5. Audit a zlepšovanie	Audit KB, kontinuálne zlepšovanie	Priebežne

Zdroj: Vlastné spracovanie

5.5.4 Záver

Piata kapitola poskytla komplexnú analýzu právneho rámca a inštitucionálnej infraštruktúry pre implementáciu technologických regulácií EÚ na Slovensku. Analýza ukázala, že Slovensko má zavedený funkčný rámec pre transpozíciu a implementáciu regulácií, pričom neprišlo k výraznému goldplatingu.

Pre malé a stredné podniky predstavujú technologické regulácie významnú záťaž, ale zároveň aj príležitosť. Podniky, ktoré úspešne implementujú požiadavky regulácií, získajú konkurenčnú výhodu v podobe vyššej dôveryhodnosti, odolnosti voči kybernetickým hrozbám a pripravenosti na digitálnu ekonomiku.

Kľúčové je pristupovať ku compliance nie ako k jednorazovej povinnosti, ale ako ku kontinuálnemu procesu zlepšovania. Regulačné prostredie sa bude naďalej vyvíjať a podniky musia byť pripravené adaptovať sa na nové požiadavky.

Nasledujúca kapitola sa zameria na praktické postupy implementácie a poskytne MSP konkrétne návody pre splnenie regulačných požiadaviek.

6 NAJZRANITEĽNEJŠIE SEGMENTY

Smernica NIS2 a jej implementácia do slovenského právneho poriadku prostredníctvom novely zákona o kybernetickej bezpečnosti menia rozsah povinností pre subjekty, ktoré pôsobia v regulovaných sektoroch alebo zabezpečujú služby dôležité pre fungovanie štátu, hospodárstva a spoločnosti. V prostredí MSP sa dopad tejto regulácie neprejavuje rovnomerne. Najvýraznejšie zasahuje tie segmenty, ktoré majú buď priamu prevádzkovú väzbu na základné alebo dôležité služby, alebo disponujú prístupom k citlivým systémom, údajom a infraštruktúre.

Tieto segmenty sú zraniteľnejšie z niekoľkých dôvodov. Po prvé, často zabezpečujú služby, ktorých výpadok by mohol mať výraznejší prevádzkový alebo spoločenský dopad. Po druhé, bývajú technicky a organizačne prepojené s väčšími regulovanými subjektmi, ktoré na ne prenášajú časť bezpečnostných a zmluvných požiadaviek. Po tretie, mnohé MSP v týchto oblastiach disponujú obmedzenými personálnymi, finančnými a odbornými kapacitami, čo sťažuje plnenie rozsiahlejších požiadaviek v oblasti riadenia rizík, dokumentácie, incident reportingu a technických opatrení.

Citeľne na ne dopadajú najmä požiadavky týkajúce sa registrácie a identifikácie postavenia podniku, zavedenia primeraných bezpečnostných opatrení, vykonávania analýzy rizík, hlásenia závažných incidentov, riadenia prístupov, kontinuity činnosti a pri niektorých subjektoch aj povinnosti preukázať súlad prostredníctvom auditu alebo samohodnotenia.

Medzi najzraniteľnejšie segmenty patria najmä podniky pôsobiace v regulovaných alebo na regulované sektory naviazaných oblastiach, predovšetkým:

- poskytovatelia IT služieb, cloudových a managed services,
- subjekty zabezpečujúce digitálnu infraštruktúru,
- dodávatelia softvéru, systémovej integrácie a technickej podpory pre regulované subjekty,
- podniky pôsobiace v energetike, doprave, zdravotníctve, elektronických komunikáciách a ďalších sektoroch osobitne vymedzených právnou úpravou,
- MSP, ktoré samy priamo nespĺňajú znaky regulovaného subjektu, ale sú súčasťou dodávateľského reťazca väčších regulovaných organizácií.

6.1 “Sebaidentifikácia” a registrácia

Každý subjekt si musí sám overiť, či spĺňa kritériá prevádzkovateľa základnej služby (PZS). Primárne sa posudzuje sektor pôsobenia podľa príloh zákona a veľkosť podniku:

- **Stredný podnik:** 50-249 zamestnancov a/alebo ročný obrat 10-50 mil. EUR
- **Veľký podnik:** 250+ zamestnancov a/alebo ročný obrat nad 50 mil. EUR
- **Výnimky:** Subjekt môže spadať pod reguláciu aj ako malý podnik, ak je jediným poskytovateľom služby v SR, predstavuje významné systémové riziko alebo je kľúčový pre verejný poriadok/bezpečnosť.

Ak subjekt spĺňa kritériá PZS, je povinný sa zaregistrovať na Národnom bezpečnostnom úrade (NBÚ):

1. Podanie oznámenia cez ústredný portál verejnej správy (slovensko.sk)
2. Lehota pre existujúce subjekty bola do 2. marca 2025
3. Pre nové subjekty platí lehota 60 dní od začatia relevantnej činnosti

4. Oznamovanie zmien zapísaných skutočností najneskôr do 14 dní.

6.2 Analýza rizík

NBÚ SR zaviedol novú metodiku analýzy rizík platnú od 1.9.2025, ktorá vychádza z medzinárodných štandardov NIST, ENISA a BSI. Metodika opisuje riadenie rizík ako cyklický proces so štyrmi hlavnými fázami.

Tab. č. 36: **Štyri hlavné fázy riadenia rizík**

Fáza	Obsah a aktivity
1. Stanovenie kontextu	Určenie prostredia, rozsahu analýzy, identifikácia kľúčových služieb a aktív organizácie
2. Analýza rizík	Identifikácia aktív, hrozieb, zraniteľností, hodnotenie pravdepodobností a dopadov
3. Ošetrenie rizík	Rozhodnutie o spôsobe nakladania s rizikom: redukcia, prenos, akceptácia alebo vyhnutie sa
4. Monitorovanie	Pravidelná aktualizácia, sledovanie a reportovanie rizík, komunikácia so stakeholdermi

Zdroj: https://www.nbu.gov.sk/data/att/3446.pdf

Organizácie si môžu zvoliť prístup, ktorý im najlepšie vyhovuje:

- **Analýza orientovaná na hrozby** – vychádza z identifikácie hrozieb a ich možných dopadov
- **Analýza orientovaná na aktíva** – sústreďuje sa na kľúčové informačné aktíva a služby
- **Analýza orientovaná na zraniteľnosti** – skúma slabiny systémov a procesov

6.3 Základné bezpečnostné opatrenia pre MSP

Implementácia bezpečnostných opatrení musí byť primeraná veľkosti a charakteru organizácie. Pre MSP odporúčame sústrediť sa na nasledujúce kľúčové oblasti:

➢ Zálohovanie a obnova dát

Pravidlo 3-2-1 predstavuje osvedčený štandard pre efektívne a spoľahlivé zálohovanie dát:

- **3 kópie dát** – redundancia je kľúčová, jedna záloha nestačí
- **2 rôzne médiá** – minimálne 2 zálohy na rozdielnych úložiskách (disk, cloud, páska)
- **1 záloha mimo lokalitu** – ochrana pred fyzickými katastrofami (požiar, povodeň, krádež)

Kritické: Pravidelne testujte obnovu zálohovaných dát. Záloha, ktorú nie je možné obnoviť, je bezcenná.

➢ Multifaktorová autentifikácia (MFA)

Multifaktorová autentifikácia je kombináciou minimálne dvoch nezávislých metód overenia identity. Implementujte MFA minimálne pre:

- Prístup do firemného e-mailu
- VPN pripojenie do firemnej siete

- Administrátorské účty a servery
- Účtovný a skladový systém
- Cloudové služby a firemné aplikácie

Aktualizácie a patch management

Bezodkladná inštalácia bezpečnostných aktualizácií je jedným z najefektívnejších opatrení. Každý MSP by mal zároveň zaviesť proces pravidelnej kontroly a aplikovania aktualizácií pre operačné systémy, aplikácie, firmvér sieťových zariadení a bezpečnostný softvér a súčasne využívať iba overené zdroje aktualizácií od oficiálnych výrobcov.

➢ Riadenie prístupových práv

Princíp minimálnych oprávnení (least privilege) zabezpečuje, že používatelia majú prístup len k dátam a systémom nevyhnutným pre ich prácu:

- Definujte roly a k nim priradené oprávnenia
- Pravidelne revidujte prístupové práva (minimálne kvartálne)
- Okamžite odoberajte prístupy pri ukončení pracovného pomeru
- Separujte administrátorské účty od bežných používateľských

6.4 Vzdelávanie a budovanie povedomia zamestnancov

Zamestnanci sú najcitlivejšou časťou kybernetickej ochrany každej firmy. Štatistiky ukazujú, že až 95 % bezpečnostných incidentov je zapríčinených ľudskou chybou a 90 % prípadov predstavuje zamestnanec vstupný bod útočníka do firemnej siete.

➢ Obsah bezpečnostného školenia

Efektívny tréningový program by mal pokrývať nasledujúce témy:

- **Rozpoznávanie phishingu** – identifikácia podozrivých e-mailov, odkazov a príloh
- **Sociálne inžinierstvo** – techniky manipulácie vrátane vishingu (telefonické podvody)
- **Bezpečnosť hesiel** – tvorba silných hesiel, používanie správcov hesiel
- **Bezpečná práca na diaľku** – pravidlá pre home office a verejné siete
- **Reakcia na incident** – komu a ako nahlásiť podozrivú aktivitu

➢ Simulované phishingové kampane

Pravidelné testovanie zamestnancov pomocou simulovaných phishingových e-mailov je účinný spôsob merania a zlepšovania bezpečnostného povedomia. Služby ako SAFELab, ESET Cybersecurity Awareness Training alebo KnowBe4 umožňujú vytvárať realistické testovacie kampane a sledovať výsledky jednotlivých zamestnancov.

6.5 Povinnosti hlásenia kybernetických incidentov

Smernica NIS2 stanovuje prísne časové rámce pre hlásenie bezpečnostných incidentov. Prevádzkovatelia základnej služby musia hlásiť každý závažný kybernetický bezpečnostný incident definovaný ako rozsiahly incident spôsobujúci alebo hroziaci závažným narušením služby.

➢ Časové lehoty hlásenia

Tab. č. 37: **Časové lehoty hlásenia**

Lehota	Typ hlásenia	Obsah
24 hodín	Včasné varovanie	Oznámenie o incidente, či bol spôsobený nezákonne, možný cezhraničný dopad
72 hodín	Oznámenie o incidente	Prvé posúdenie závažnosti a dopadov, indikátory kompromitácie
30 dní	Záverečná správa	Kompletná správa o incidente, príčiny, dopady, prijaté opatrenia

Zdroj: Smernica (EÚ) 2022/2555 Európskeho parlamentu a Rady zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2). Úradný vestník Európskej únie

➢ Komu hlásiť incidenty

Hlásenia sa podávajú Národnému bezpečnostnému úradu (NBÚ) alebo príslušnej národnej jednotke CSIRT (Computer Security Incident Response Team). Každý členský štát má určený jednotný kontaktný bod pre nahlasovanie bezpečnostných incidentov.

6.6 ISO 27001 a vzťah k NIS2

Medzinárodná norma ISO/IEC 27001 špecifikuje požiadavky na systém manažérstva informačnej bezpečnosti (ISMS) a poskytuje systematický rámec pre implementáciu bezpečnostných opatrení. Certifikácia podľa ISO 27001 môže výrazne uľahčiť dosiahnutie súladu s NIS2.

Výhody implementácie ISO 27001:

- Systematický prístup k riadeniu informačnej bezpečnosti
- Zvýšenie dôveryhodnosti voči zákazníkom a partnerom
- Konkurenčná výhoda pri výberových konaniach
- Súlad s legislatívnymi požiadavkami (NIS2, GDPR)
- Zníženie rizika bezpečnostných incidentov a súvisiacich nákladov

Kroky k certifikácii:

1. **Analýza súčasného stavu** – gap analýza voči požiadavkám normy
2. **Vybudovanie ISMS** – vypracovanie dokumentácie a zavedenie procesov
3. **Interný audit** – overenie správnosti implementácie
4. **Certifikačný audit** – nezávislý certifikačný orgán overí splnenie požiadaviek
5. **Udržiavanie a zlepšovanie** – pravidelné dozorné audity a kontinuálne zlepšovanie

6.7 Praktické rady pre MSP

➢ Prioritizácia opatrení

Pri limitovaných zdrojoch je dôležité začať od najkritickejších oblastí:

1. **Zálohovanie (pravidlo 3-2-1)** – základ pre obnovu po akomkoľvek incidente

2. **MFA na kritických systémoch** – e-mail, VPN, administrácia
3. **Aktualizácie** – automatizácia kde je to možné
4. **Školenie zamestnancov** – najslabší článok reťazca
5. **Plán reakcie na incidenty** – vedieť čo robiť keď sa niečo stane

- Externá podpora

Pre firmy bez dostatočných interných kapacít je vhodné zvážiť outsourcing bezpečnostných služieb. Managed Security Service Providers (MSSP) ponúkajú monitoring 24/7, správu bezpečnostných zariadení, reakciu na incidenty a pomoc s compliance. Táto možnosť môže byť pre MSP nákladovo efektívnejšia ako budovanie vlastného bezpečnostného tímu.

- Dokumentácia

Nie je cieľom mať stovky dokumentov. Sústreďte sa na kľúčovú dokumentáciu: Politiku kybernetickej bezpečnosti, Analýzu rizík, Plán kontinuity podnikania (BCP), Plán obnovy po havárii (DRP), Záznamy o školeniach a Evidenciu incidentov. Dokumentácia musí byť aktuálna a prístupná zodpovedným osobám.

6.8 Sankcie za nedodržanie požiadaviek

Zákon stanovuje prísne sankcie za porušenie povinností. Je dôležité si uvedomiť, že konatelia a manažéri nesú osobnú zodpovednosť za zabezpečenie primeraných opatrení - kybernetická bezpečnosť nie je len IT téma.

Tab. č. 38: **Typ porušenia a výška pokuty**

Typ porušenia	Výška pokuty
Neoznámenie začiatku činnosti, neohlásenie zmien, neaktuálna dokumentácia	300 € až 500 000 €
Neplnenie bezpečnostných opatrení, nehlásenie incidentov (dôležité subjekty)	až 7 000 000 € alebo 1,4% obratu
Závažné porušenia (kľúčové subjekty)	až 10 000 000 € alebo 2% obratu

Zdroj: Zákon o kybernetickej bezpečnosti

6.9 Záver a kľúčové termíny

Implementácia požiadaviek NIS2 je náročný, ale zvládnuteľný proces. Kľúčom k úspechu je systematický prístup, prioritizácia kritických opatrení a dodržanie zákonných termínov. Pamätajte, že kybernetická bezpečnosť je kontinuálny proces, nie jednorazový projekt.

Kľúčové termíny

1. **Január 2025:** Účinnosť novely zákona o kybernetickej bezpečnosti
2. **12 mesiacov od registrácie:** Lehota na implementáciu bezpečnostných opatrení
3. **Marec 2026:** Deadline pre zavedenie bezpečnostných opatrení
4. **Marec 2027:** Povinnosť vykonania prvého auditu alebo samohodnotenia
5. **September 2025:** Účinnosť novej metodiky analýzy rizík NBÚ

7 NÁVRHY ODPORÚČANÍ A PODPORNÝCH OPATRENÍ ZO STRANY ŠTÁTU

Implementácia technologických regulácií EÚ – AI Act, Cyber Resilience Act a smernice NIS2 – predstavuje pre malé a stredné podniky na Slovensku komplexnú výzvu, ktorá si vyžaduje aktívnu podporu zo strany štátu. Na základe analýzy priamych a nepriamych dopadov regulácií, identifikovaných bariér a medzinárodných skúseností táto kapitola predkladá konkrétne návrhy odporúčaní a podporných opatrení, ktoré by mohli zmierniť negatívne dopady regulácií na MSP a súčasne maximalizovať príležitosti, ktoré tieto regulácie prinášajú.

Návrhy sú štruktúrované do piatich oblastí: metodická a informačná podpora, finančné a ekonomické nástroje, legislatívna a regulačná podpora, vzdelávanie a budovanie kapacít a iné druhy podpory. Pre každú oblasť sú identifikované konkrétne opatrenia, zodpovedné inštitúcie a odporúčané termíny implementácie.

7.1 Metodická a informačná podpora

Jednou z najvýznamnejších bariér pre MSP pri implementácii nových regulácií je nedostatok zrozumiteľných a praktických informácií. Prieskumy opakovane ukazujú, že MSP majú obmedzené kapacity na sledovanie legislatívneho vývoja a interpretáciu komplexných právnych predpisov. Štát preto musí zohrávať aktívnu úlohu pri sprístupňovaní informácií a metodickej podpory.

7.1.1 Jednotný informačný portál pre technologické regulácie

Základným predpokladom úspešnej implementácie regulácií je vytvorenie jednotného, centralizovaného informačného portálu, ktorý bude slúžiť ako primárny zdroj informácií pre MSP o všetkých relevantných technologických reguláciách EÚ. Portál by mal integrovať informácie o AI Act, CRA a NIS2 na jednom mieste a poskytnúť MSP komplexný prehľad o ich povinnostiach.

Kľúčové funkcie portálu:

- Interaktívny nástroj na sebahodnotenie, ktorý MSP umožní identifikovať, ktoré regulácie a povinnosti sa na nich vzťahujú
- Databáza často kladených otázok (FAQ) s praktickými príkladmi a odpoveďami na najčastejšie dotazy
- Vzorová dokumentácia a šablóny (analýza rizík, bezpečnostná dokumentácia, SBOM, technická dokumentácia AI systémov)
- Kalendár kľúčových termínov a míľnikov s možnosťou notifikácií
- Adresár certifikovaných poskytovateľov služieb v oblasti compliance, kybernetickej bezpečnosti a AI
- Prehľad dostupných finančných nástrojov a grantových výziev

Portál by mal byť prevádzkovaný v spolupráci Slovak Business Agency, Ministerstva investícií, regionálneho rozvoja a informatizácie SR (MIRRI) a Národného bezpečnostného úradu (NBÚ). Odporúčaný termín spustenia základnej verzie portálu je prvý kvartál 2026, s postupným rozširovaním funkcionalít.

7.1.2 Metodické usmernenia a príručky pre MSP

Okrem centrálneho portálu je potrebné vypracovať sadu špecializovaných metodických materiálov, ktoré budú MSP viesť procesom dosiahnutia súladu s jednotlivými reguláciami. Tieto materiály by mali byť písané zrozumiteľným jazykom, orientované na praktické kroky a doplnené o konkrétne príklady z praxe.

Odporúčané metodické materiály:

1. **Príručka pre MSP k AI Act** – praktický sprievodca klasifikáciou AI systémov, povinnosťami poskytovateľov a nasadzovateľov, s osobitným dôrazom na vysokorizikové systémy a požiadavky na AI gramotnosť
2. **Príručka pre MSP k CRA** – návod na implementáciu požiadaviek na kybernetickú bezpečnosť produktov s digitálnymi prvkami, vrátane tvorby SBOM a procesov hlásenia zraniteľností
3. **Príručka pre MSP k NIS2** – sprievodca povinnosťami prevádzkovateľov základnej služby a dôležitých subjektov podľa novely zákona o kybernetickej bezpečnosti
4. **Vzorová bezpečnostná dokumentácia** – kompletný balík vzorových dokumentov v súlade s vyhláškou NBÚ č. 362/2018 Z. z., upravený pre potreby MSP
5. **Metodika analýzy rizík pre MSP** – zjednodušená metodika analýzy rizík prispôsobená kapacitám a potrebám menších podnikov

Tieto materiály by mali byť vypracované v spolupráci s NBÚ, MIRRI a odbornými asociáciami (IT Asociácia Slovenska, Slovenská obchodná a priemyselná komora) a pravidelne aktualizované v súlade s vývojom regulácií a ich výkladov.

7.1.3 Helpdesk a poradenské služby

Pre MSP s obmedzenými internými kapacitami je dôležité zabezpečiť prístup k individuálnemu poradenstvu. Na európskej úrovni AI Act predpokladá, že Európske centrá digitálnych inovácií (EDIH) budú od roku 2025 fungovať ako AI helpdesky poskytujúce poradenstvo k otázkam súvisiacim s AI Act. Na Slovensku pôsobí päť EDIH, ktoré by mali túto funkciu plniť.

Odporúčané opatrenia:

- Rozšírenie kapacít slovenských EDIH na poskytovanie komplexného poradenstva nielen k AI Act, ale aj k CRA a NIS2
- Zriadenie telefonickej linky a e-mailovej podpory pre základné otázky MSP k technologickým reguláciám
- Poskytovanie bezplatných úvodných konzultácií (napríklad 2 hodiny) pre MSP na posúdenie ich regulačnej expozície
- Organizovanie pravidelných webinárov a Q&A sessions s expertmi na jednotlivé regulácie

Tab. č. 39: **Prehľad EDIH na Slovensku a ich zameranie**

EDIH	Zameranie	Webová stránka
HOPERO	Umelá inteligencia, inovatívna ekonomika	hopero.sk
CASSOVIUM	AI, Industry 4.0, kybernetická bezpečnosť (východné Slovensko)	edihcassovium.sk
HealthHub	Digitalizácia a inovácie v zdravotníctve	healthhub.sk
EXPANDI 4.0	Digitalizácia priemyselných MSP	expandi40.sk
SCDI	Industry 4.0, kybernetická bezpečnosť, smart energetika	scdi.tech

Zdroj: MIRRI SR, edihslovensko.sk

7.2 Finančné a ekonomické nástroje

Analýza v predchádzajúcich kapitolách ukázala, že náklady na dosiahnutie súladu s novými reguláciami môžu pre MSP predstavovať 0,8 až 1,9 % obratu. Pre mikropodniky a malé podniky s obmedzenými finančnými zdrojmi môže táto záťaž ohroziť ich konkurencieschopnosť alebo dokonca existenciu. Štát preto musí poskytnúť adekvátne finančné nástroje na zmiernenie týchto dopadov.

7.2.1 Grantové schémy na podporu compliance

Jedným z najefektívnejších nástrojov podpory MSP sú cielené grantové schémy, ktoré umožňujú čiastočné preplatenie nákladov na dosiahnutie súladu s reguláciami. Príkladom úspešnej iniciatívy je výzva Kompetenčného a certifikačného centra kybernetickej bezpečnosti (NCC-SK) z roku 2024, ktorá podporila vypracovanie bezpečnostnej dokumentácie pre MSP grantom až do výšky 90 % oprávnených nákladov.

Odporúčané grantové schémy:

1. **Grant na kybernetickú bezpečnosť pre MSP** – pokračovanie a rozšírenie existujúcej výzvy NCC-SK s rozšíreným rozsahom oprávnených aktivít (bezpečnostná dokumentácia, penetračné testy, implementácia bezpečnostných opatrení, školenia). Odporúčaná alokácia: minimálne 10 miliónov EUR ročne.
2. **Grant na AI compliance** – nová grantová schéma na podporu MSP pri implementácii požiadaviek AI Act, vrátane vypracovania technickej dokumentácie, posúdenia zhody a úprav AI systémov. Odporúčaná alokácia: 5 miliónov EUR ročne.
3. **Grant na certifikáciu ISO 27001** – podpora pre MSP na získanie certifikácie podľa ISO/IEC 27001, ktorá uľahčuje preukázanie súladu s NIS2 a buduje dôveru voči zákazníkom. Odporúčaná alokácia: 3 milióny EUR ročne.
4. **Inovačné vouchery na digitálnu bezpečnosť** – poukážky v hodnote 5 000 – 15 000 EUR na nákup služieb v oblasti kybernetickej bezpečnosti a AI compliance od akreditovaných poskytovateľov.

Finančné prostriedky na tieto schémy by mali byť zabezpečené z Plánu obnovy a odolnosti SR, programu Digitálna Európa, Programu Slovensko 2021–2027 a z národných zdrojov prostredníctvom rozpočtových kapitol relevantných ministerstiev.

7.2.2 Zvýhodnené úvery a záruky

Pre MSP, ktoré potrebujú väčšie investície do technológií a infraštruktúry, môžu byť vhodnejšie návratné formy financovania. Slovak Investment Holding (SIH) a Fond inovácií a technológií (FIT) by mali rozšíriť svoje portfólio o produkty zamerané na podporu digitálnej bezpečnosti.

Odporúčané finančné nástroje:

- **Zvýhodnený úver na kybernetickú bezpečnosť** – úver s úrokovou sadzbou pod úrovňou trhu na financovanie bezpečnostných technológií, softvéru a služieb
- **Záručná schéma pre MSP** – štátna záruka za komerčné úvery na digitalizáciu a kybernetickú bezpečnosť, čím sa zníži úrokové zaťaženie a zlepší prístup k financovaniu
- **Mikropôžičky na compliance** – program mikropôžičiek do 25 000 EUR s minimálnou administratívnou záťažou pre mikropodniky.

7.2.3 Daňové stimuly

Daňové stimuly môžu motivovať MSP k proaktívnym investíciám do bezpečnosti a compliance bez potreby zložitého procesu žiadania o granty.

Odporúčané daňové opatrenia:

- **Superodpočet na kybernetickú bezpečnosť** – rozšírenie existujúceho superodpočtu na výskum a vývoj o položky súvisiace s implementáciou bezpečnostných opatrení a AI compliance
- **Zrýchlené odpisy** – umožnenie zrýchleného odpisovania investícií do bezpečnostných technológií (hardvér, softvér)
- **Oslobodenie od DPH** – zváženie oslobodenia od DPH pre certifikačné služby a bezpečnostné audity poskytované MSP.

Tab. č. 40: **Prehľad odporúčaných finančných nástrojov**

Nástroj	Forma podpory	Cieľová skupina	Odporúčaná alokácia
Grant na kybernetickú bezpečnosť	Nenávratná dotácia (až 90 %)	Všetky MSP	10 mil. EUR/rok
Grant na AI compliance	Nenávratná dotácia (až 80 %)	MSP vyvíjajúce/nasadzujúce AI	5 mil. EUR/rok
Grant na ISO 27001	Nenávratná dotácia (až 70 %)	Stredné podniky	3 mil. EUR/rok
Inovačné vouchery	Poukážka 5–15 tis. EUR	Mikro a malé podniky	2 mil. EUR/rok
Zvýhodnený úver SIH	Návratné financovanie	Všetky MSP	20 mil. EUR

Zdroj: Vlastné spracovanie

7.3 Legislatívna a regulačná podpora

Okrem informačnej a finančnej podpory je dôležité, aby legislatívny a regulačný rámec na národnej úrovni bol nastavený spôsobom, ktorý minimalizuje administratívnu záťaž pre MSP a maximalizuje právnu istotu.

7.3.1 Zriadenie a prevádzka regulačného sandboxu pre AI

AI Act v článku 57 ukladá každému členskému štátu povinnosť zriadiť aspoň jeden regulačný sandbox na národnej úrovni, ktorý musí byť funkčný do 2. augusta 2026. Regulačné sandboxy poskytujú kontrolované prostredie, kde môžu MSP a startupy vyvíjať a testovať inovatívne AI systémy pod dohľadom regulátora, s právnou istotou a ochranou pred pokutami počas obdobia účasti v sandboxe.

Odporúčania pre slovenský regulačný sandbox:

- **Včasné zriadenie -** Spustiť prevádzku sandboxu najneskôr do júla 2026, ako avizovalo MIRRI
- **Prioritný prístup pre MSP -** V súlade s AI Act zabezpečiť prioritný prístup pre MSP a startupy
- **Bezplatná účasť -** Účasť v sandboxe by mala byť pre MSP bezplatná alebo s minimálnymi poplatkami
- **Jasné pravidlá -** Vypracovať transparentné pravidlá účasti, kritériá prijatia a výstupov zo sandboxu
- **Prepojenie s EDIH -** Integrovať sandbox s aktivitami slovenských EDIH a poskytnúť komplexnú podporu účastníkom.

Zodpovedným orgánom za zriadenie a prevádzku sandboxu by mal byť úrad určený ako príslušný orgán pre AI Act na Slovensku, pravdepodobne v koordinácii s MIRRI a splnomocnencom vlády pre umelú inteligenciu.

7.3.2 Proporcionálny prístup k dohľadu a sankciám

Pri výkone dohľadu a ukladaní sankcií je potrebné zohľadňovať veľkosť a kapacity MSP. Regulácie samotné obsahujú určité mechanizmy proporcionality, avšak ich praktická aplikácia závisí od prístupu národných orgánov.

Odporúčania:

- **Prechodné obdobie benevolencie:** V prvých 12–18 mesiacoch po nadobudnutí účinnosti jednotlivých povinností uplatňovať voči MSP primárne poradenský a nápravný prístup namiesto sankcií
- **Varovné mechanizmy:** Pred uložením sankcie vždy poskytnúť MSP varovanie a primeranú lehotu na nápravu (s výnimkou závažných porušení)
- **Zohľadnenie veľkosti:** Pri stanovení výšky pokút dôsledne zohľadňovať finančnú situáciu MSP a uplatňovať nižšie sadzby v súlade s ustanoveniami regulácií
- **Jasné usmernenia:** NBÚ a ďalšie dohľadové orgány by mali vydať usmernenia objasňujúce, ako budú pristupovať k dohľadu nad MSP.

7.3.3 Zjednodušená dokumentácia pre MSP

AI Act v článku 63 umožňuje príslušným orgánom povoliť MSP zjednodušenú formu technickej dokumentácie pre vysokorizikové AI systémy. Táto možnosť by mala byť aktívne využívaná a podporovaná.

Odporúčania:

- Vypracovať a zverejniť vzory zjednodušenej technickej dokumentácie pre najčastejšie typy vysokorizikových AI systémov vyvíjaných MSP
- Poskytnúť jasné kritériá, kedy a za akých podmienok môžu MSP využiť zjednodušenú dokumentáciu
- Zabezpečiť, aby zjednodušená dokumentácia bola uznávaná aj pre účely posúdenia zhody.

7.4 Vzdelávanie a budovanie kapacít

Nedostatok kvalifikovaných odborníkov v oblasti kybernetickej bezpečnosti a AI predstavuje jednu z najvýznamnejších bariér pre implementáciu regulácií. Podľa prieskumu ENISA až 89 % organizácií očakáva potrebu dodatočných zamestnancov a 59 % MSP hlási ťažkosti s obsadzovaním pozícií v kybernetickej bezpečnosti. Systematické budovanie kapacít je preto nevyhnutné.

7.4.1 Vzdelávacie programy pre MSP

Odporúčané vzdelávacie aktivity:

1. **Séria bezplatných webinárov** – pravidelné online semináre k jednotlivým aspektom AI Act, CRA a NIS2, organizované EDIH, SBA a odbornými asociáciami
2. **Certifikované kurzy** – štandardizované kurzy AI gramotnosti a kybernetickej bezpečnosti pre zamestnancov MSP, ukončené certifikátom
3. **Workshopy a bootcampy** – intenzívne praktické workshopy zamerané na konkrétne témy (tvorba SBOM, analýza rizík, reakcia na incidenty)
4. **E-learningová platforma** – vytvorenie online platformy s kurzami k technologickým reguláciám, dostupnej zadarmo alebo za symbolický poplatok
5. **Mentoring program** – prepojenie MSP bez skúseností s compliance s podnikmi, ktoré už úspešne implementovali požiadavky regulácií.

7.4.2 Podpora AI gramotnosti

AI Act v článku 4 stanovuje povinnosť zabezpečiť dostatočnú úroveň AI gramotnosti zamestnancov, ktorí pracujú s AI systémami. Táto povinnosť nadobudla účinnosť 2. februára 2025 a vzťahuje sa na všetky podniky využívajúce AI, bez ohľadu na ich veľkosť.

Odporúčané opatrenia:

- Vypracovať národné usmernenie k požiadavkám na AI gramotnosť vrátane odporúčaného obsahu školení a spôsobov dokumentácie
- Poskytnúť bezplatné online kurzy AI gramotnosti pre zamestnancov MSP prostredníctvom EDIH a Digitálnej koalície
- Zahrnúť AI gramotnosť do programov rekvalifikácie podporovaných úradmi práce

- Podporiť vznik certifikačnej schémy AI gramotnosti uznávanej na národnej úrovni.

7.4.3 Rozvoj kapacít v kybernetickej bezpečnosti

Globálny deficit odborníkov na kybernetickú bezpečnosť dosahuje podľa odhadov 3,4 milióna. Pre Slovensko je nevyhnutné systematicky budovať pipeline talentov v tejto oblasti.

Dlhodobé opatrenia:

- Posilnenie výučby kybernetickej bezpečnosti na stredných odborných školách a vysokých školách
- Podpora certifikačných programov (CISSP, CISM, CompTIA Security+) pre záujemcov o kariéru v kybernetickej bezpečnosti
- Rekvalifikačné programy pre pracovníkov z iných IT oblastí
- Spolupráca so zahraničnými univerzitami a certifikačnými orgánmi
- Podpora účasti slovenských odborníkov na medzinárodných konferenciách a školeniach.

7.5 Iné druhy podpory

Okrem metodickej, finančnej, legislatívnej a vzdelávacej podpory existujú ďalšie oblasti, kde štát môže prispieť k úspešnej implementácii technologických regulácií zo strany MSP.

7.5.1 Podpora spolupráce a networkingu

MSP môžu významne profitovať zo vzájomnej spolupráce a zdieľania skúseností. Štát by mal aktívne podporovať vytváranie sietí a komunít zameraných na technologické regulácie.

Odporúčané aktivity:

1. **Sektorové pracovné skupiny** – vytvorenie pracovných skupín pre kľúčové sektory (IT, výroba, finančné služby, zdravotníctvo), kde budú MSP zdieľať skúsenosti a best practices
2. **Konferencie a podujatia** – organizovanie pravidelných konferencií k technologickým reguláciám s účasťou domácich aj zahraničných expertov
3. **Online komunity** – podpora vzniku online fór a komunít pre výmenu informácií medzi MSP
4. **Medzinárodná spolupráca** – prepojenie slovenských MSP so zahraničnými partnermi prostredníctvom siete Enterprise Europe Network a medzinárodných programov.

7.5.2 Zdieľané služby a kolektívne riešenia

Pre MSP s obmedzenými zdrojmi môžu byť nákladovo efektívne zdieľané riešenia a kolektívne služby.

Odporúčania:

- **Zdieľaný CISO/DPO** – podpora modelov zdieľaného odborníka na kybernetickú bezpečnosť alebo ochranu údajov pre skupiny MSP

- **Kolektívne poistenie** – facilitácia vzniku skupinových produktov kybernetického poistenia pre MSP s výhodnejšími podmienkami
- **Spoločné bezpečnostné operačné centrum (SOC)** – podpora vzniku zdieľaného SOC pre MSP, ktoré si nemôžu dovoliť vlastné kapacity 24/7 monitoringu
- **Rámcové zmluvy s poskytovateľmi** – vyjednanie rámcových zmlúv so zvýhodnenými cenami pre MSP na služby v oblasti compliance a bezpečnosti.

7.5.3 Podpora exportu a medzinárodnej expanzie

Compliance s európskymi reguláciami môže byť konkurenčnou výhodou na globálnych trhoch vďaka tzv. Bruselskému efektu. Štát by mal podporiť MSP v kapitalizácii tejto výhody.

Odporúčania:

- Zahrnutie compliance s AI Act a CRA do marketingových materiálov pre podporu exportu
- Podpora účasti slovenských MSP na medzinárodných veľtrhoch a obchodných misiách zameraných na digitálne technológie
- Poskytovanie informácií o regulačných požiadavkách na kľúčových exportných trhoch mimo EÚ.

Tab. č. 41: **Súhrnný prehľad odporúčaných opatrení a zodpovedných inštitúcií**

Oblasť podpory	Kľúčové opatrenia	Zodpovedné inštitúcie
7.1 Metodická a informačná podpora	Jednotný portál, príručky, helpdesk	SBA, MIRRI, NBÚ, EDIH
7.2 Finančné a ekonomické nástroje	Granty, úvery, vouchery, dane	MH SR, MF SR, SIH, NCC-SK
7.3 Legislatívna a regulačná podpora	Sandbox, proporcionálny dohľad	MIRRI, NBÚ, Splnomocnenec pre AI
7.4 Vzdelávanie a budovanie kapacít	Kurzy, certifikácie, AI gramotnosť	EDIH, MŠ SR, Digitálna koalícia
7.5 Iné druhy podpory	Networking, zdieľané služby, export	SBA, SOPK, SARIO, EEN

Zdroj: Vlastné spracovanie

7.6 Zhrnutie a prioritizácia opatrení

Úspešná implementácia technologických regulácií EÚ zo strany slovenských MSP si vyžaduje komplexný prístup zo strany štátu. Navrhované opatrenia v tejto kapitole tvoria vzájomne prepojený systém podpory, ktorý pokrýva informačné, finančné, legislatívne, vzdelávacie a ďalšie potreby MSP.

Prioritné opatrenia s najvyšším dopadom:

1. **Spustenie jednotného informačného portálu** – základný predpoklad pre informovanosť MSP, odporúčaný termín Q1/2026
2. **Pokračovanie a rozšírenie grantovej schémy na kybernetickú bezpečnosť** – priama finančná pomoc s najrýchlejším dopadom
3. **Zriadenie regulačného sandboxu pre AI** – kľúčové pre inovatívne MSP vyvíjajúce AI systémy, povinný termín august 2026

4. **Rozšírenie kapacít EDIH na AI helpdesk** – priame poradenstvo pre MSP k AI Act
5. **Programy AI gramotnosti** – urgentná potreba vzhľadom na účinnosť povinnosti od februára 2025

Realizácia týchto opatrení vyžaduje koordinovaný prístup viacerých inštitúcií a adekvátne finančné zabezpečenie. Odporúčame vytvorenie medzirezortnej pracovnej skupiny pre podporu MSP pri implementácii technologických regulácií, ktorá by koordinovala aktivity jednotlivých rezortov a inštitúcií a pravidelne vyhodnocovala účinnosť podporných opatrení.

Celková odporúčaná alokácia finančných prostriedkov na podporné opatrenia pre MSP v oblasti technologických regulácií je minimálne 25 miliónov EUR ročne, s čerpaním primárne z Plánu obnovy a odolnosti SR, programu Digitálna Európa a Programu Slovensko 2021–2027. Tieto prostriedky predstavujú investíciu do konkurencieschopnosti slovenského podnikateľského prostredia a dlhodobej odolnosti slovenskej ekonomiky v digitálnej ére.

8 ZÁVERY A ODPORÚČANIA PRE MSP

Predchádzajúce kapitoly tejto analýzy poskytli komplexný prehľad o troch kľúčových technologických reguláciách Európskej únie – AI Act, Cyber Resilience Act a smernici NIS2 – a ich dopadoch na malé a stredné podniky na Slovensku. Táto kapitola syntetizuje hlavné zistenia analýzy a formuluje praktické odporúčania pre samotné MSP, ktoré im pomôžu úspešne sa orientovať v novom regulačnom prostredí a využiť príležitosti, ktoré regulácie prinášajú.

Odporúčania sú štruktúrované chronologicky podľa fáz prípravy na regulácie a následne tematicky podľa jednotlivých oblastí. Cieľom je poskytnúť MSP praktický návod, ktorý môžu bezprostredne využiť pri plánovaní a implementácii svojej compliance stratégie.

8.1 Syntéza kľúčových zistení analýzy

Analýza identifikovala niekoľko kľúčových zistení, ktoré sú relevantné pre všetky MSP bez ohľadu na ich veľkosť, sektor či mieru priamej regulačnej expozície.

8.1.1 Rozsah a záväznosť regulácií

Technologické regulácie EÚ predstavujú najkomplexnejší regulačný rámec pre digitálne technológie na svete. Na rozdiel od predchádzajúcich regulácií, ktoré sa zameriavali primárne na veľké podniky, nové regulácie majú širší dosah a ovplyvňujú MSP v rôznych rolách – ako poskytovateľov a nasadzovateľov AI systémov, výrobcov produktov s digitálnymi prvkami, dodávateľov regulovaných subjektov a prevádzkovateľov základných služieb.

Kľúčové fakty:

- AI Act sa vzťahuje na všetky podniky vyvíjajúce alebo používajúce AI systémy v EÚ, bez ohľadu na ich veľkosť
- CRA pokrýva prakticky všetky produkty s digitálnymi prvkami uvádzané na trh EÚ
- NIS2 sa priamo vzťahuje na stredné a veľké podniky v 16 regulovaných odvetviach, ale nepriamo ovplyvňuje aj ich dodávateľov
- Podľa dôvodovej správy sa novela zákona o kybernetickej bezpečnosti dotýka minimálne 3 403 organizácií na Slovensku.

8.1.2 Náklady a prínosy compliance

Analýza ukázala, že náklady na dosiahnutie súladu s novými reguláciami môžu pre MSP predstavovať 0,8 až 1,9 % ročného obratu, v závislosti od veľkosti podniku a miery regulačnej expozície. Tieto náklady zahŕňajú jednorazové investície do technológií a procesov, priebežné náklady na údržbu a aktualizácie, náklady na špecializovaný personál alebo externé služby a náklady na certifikáciu a audity.

Súčasne však analýza identifikovala významné prínosy compliance: prístup na jednotný trh EÚ s viac ako 450 miliónmi spotrebiteľov, zvýšenie dôvery zákazníkov a obchodných partnerov, zníženie rizika kybernetických incidentov a súvisiacich nákladov, konkurenčnú výhodu v dodávateľských reťazcoch a možnosť využitia Bruselského efektu pri expanzii na globálne trhy.

8.1.3 Diferenciácia dopadov podľa typu MSP

Dopady regulácií nie sú rovnomerné naprieč všetkými MSP. Analýza identifikovala niekoľko segmentov s rôznou mierou dotknutosti:

Najviac dotknuté segmenty:

- Poskytovatelia vysokorizikových AI systémov (HR tech, fintech, healthtech, EdTech)
- Výrobcovia IoT zariadení a softvérových produktov
- Stredné podniky v sektoroch regulovaných NIS2 (energetika, doprava, zdravotníctvo, digitálna infraštruktúra)
- Dodávatelia kritických komponentov pre veľké podniky

Menej priamo dotknuté segmenty:

- Mikropodniky a malé podniky mimo regulovaných sektorov
- Poskytovatelia tradičných služieb bez významnej digitálnej zložky
- Podniky pôsobiace výlučne na lokálnom trhu bez ambície expanzie

Tab. č. 42: **Kľúčové termíny účinnosti regulácií**

Regulácia	Povinnosť	Termín
AI Act	Zákaz neprijateľných AI praktík	2. február 2025
AI Act	Povinnosť AI gramotnosti zamestnancov	2. február 2025
AI Act	Pravidlá pre GPAI modely	2. august 2025
AI Act	Plná účinnosť (vysokorizikové AI)	2. august 2026
NIS2	Účinnosť novely zákona o KB	1. január 2025
NIS2	Implementácia bezpečnostných opatrení	Marec 2026
NIS2	Prvý audit/samohodnotenie	Marec 2027
CRA	Hlásenie zraniteľností ENISA	11. september 2026
CRA	Plná účinnosť hlavných povinností	11. december 2027

Zdroj: AI Act, CRA, zákon č. 366/2024 Z. z.

8.2 Strategické odporúčania pre MSP

Na základe zistení analýzy formulujeme nasledujúce strategické odporúčania, ktoré by mali MSP zohľadniť pri formulovaní svojho prístupu k technologickým reguláciám.

8.2.1 Vykonajte sebahodnotenie regulačnej expozície

Prvým a nevyhnutným krokom pre každé MSP je dôkladné posúdenie, ktoré regulácie a v akom rozsahu sa na podnik vzťahujú. Mnohé MSP podcenia túto fázu a buď zbytočne investujú do compliance v oblastiach, ktoré sa ich netýkajú, alebo naopak prehliadnu povinnosti, ktorým podliehajú.

Otázky pre sebahodnotenie:

1. **AI Act:** Vyvíjame, uvádzame na trh alebo používame AI systémy? Ak áno, do akej rizikovej kategórie spadajú?

2. **CRA:** Vyrábame, dovážame alebo distribuujeme produkty s digitálnymi prvkami (hardvér alebo softvér)?
3. **NIS2:** Pôsobíme v niektorom z 16 regulovaných sektorov a spĺňame veľkostné kritériá (50+ zamestnancov alebo obrat nad 10 mil. EUR)?
4. **Dodávateľský reťazec:** Sme dodávateľom pre veľké podniky alebo subjekty regulované NIS2?

Pre MSP bez interných kapacít na takéto hodnotenie odporúčame využiť bezplatné konzultácie poskytované EDIH alebo služby špecializovaných poradcov.

8.2.2 Zvoľte explicitnú strategickú pozíciu

Na základe výsledkov sebahodnotenia by malo každé MSP zvoliť jednu zo štyroch strategických pozícií identifikovaných v analýze. Táto voľba by mala byť vedomá, zdokumentovaná a komunikovaná v rámci organizácie.

Štyri strategické pozície:

1. **Líder:** Pre MSP s vysokou regulačnou expozíciou a dostatočnými zdrojmi, ktoré chcú využiť compliance ako konkurenčnú výhodu
2. **Rýchly nasledovník:** Pre väčšinu MSP v regulovaných oblastiach – včasná, ale nie predčasná implementácia
3. **Minimalistický adaptér:** Pre MSP s nízkou priamou expozíciou – splnenie minimálnych požiadaviek
4. **Strategický exiter:** Pre MSP, kde náklady compliance prevyšujú prínosy – zváženie opustenia regulovanej oblasti

8.2.3 Integrujte compliance do podnikovej stratégie

Compliance by nemalo byť izolovaným projektom, ale integrálnou súčasťou podnikovej stratégie. MSP, ktoré vnímajú compliance len ako náklad a administratívnu záťaž, premrhajú príležitosť transformovať regulačné požiadavky na konkurenčnú výhodu.

Praktické kroky integrácie:

- Zahrňte compliance do produktovej stratégie – bezpečnosť a transparentnosť ako súčasť hodnoty pre zákazníka
- Komunikujte compliance voči zákazníkom a partnerom ako diferenciačný faktor
- Využite compliance požiadavky na optimalizáciu interných procesov
- Hľadajte synergické efekty – jedno opatrenie môže splniť požiadavky viacerých regulácií

8.3 Praktické kroky implementácie

Táto časť poskytuje konkrétne praktické kroky, ktoré by MSP mali podniknúť na dosiahnutie súladu s jednotlivými reguláciami.

8.3.1 Kroky pre súlad s AI Act

Pre nasadzovateľov AI systémov (všetky MSP používajúce AI):

1. Zabezpečte AI gramotnosť zamestnancov (povinnosť od 2. februára 2025). Identifikujte zamestnancov pracujúcich s AI systémami a zabezpečte im adekvátne školenie o fungovaní AI, jej obmedzeniach a správnom používaní.
2. Vykonajte inventarizáciu AI systémov**.** Zmapujte všetky AI systémy používané v podniku, vrátane cloudových služieb tretích strán.
3. Klasifikujte AI systémy podľa rizika. Určte, či niektoré z vašich AI systémov spadajú do kategórie vysokorizikových podľa Prílohy III AI Act.
4. Pre vysokorizikové AI systémy zabezpečte ľudský dohľad, uchovávajte logy vstupných údajov a vykonajte hodnotenie vplyvu na základné práva (ak je vyžadované).
5. Pre systémy s obmedzeným rizikom zabezpečte transparentnosť voči používateľom (napríklad informovanie, že komunikujú s AI).

Pre poskytovateľov vysokorizikových AI systémov:

1. Zavedenie systému riadenia kvality (QMS) pokrývajúceho celý životný cyklus AI systému
2. Vypracovanie technickej dokumentácie v súlade s požiadavkami AI Act
3. Vykonanie posúdenia zhody (interné alebo treťou stranou podľa typu systému)
4. Registrácia v databáze EÚ pred uvedením na trh
5. Zavedenie systému monitorovania po uvedení na trh
6. Zváženie účasti v regulačnom sandboxe (po jeho zriadení na Slovensku)

8.3.2 Kroky pre súlad s CRA

Pre výrobcov produktov s digitálnymi prvkami:

1. Implementujte princípy security by design a security by default do vývojového procesu – bezpečnosť musí byť integrovaná od počiatku, nie pridaná dodatočne.
2. Vytvorte SBOM – detailný zoznam všetkých softvérových komponentov vrátane open-source závislostí.
3. Zavedenie procesu správy zraniteľností – schopnosť identifikovať, hodnotiť a riešiť bezpečnostné zraniteľnosti počas celého životného cyklu produktu.
4. Pripravte sa na hlásenie zraniteľností (od septembra 2026) – aktívne zneužívané zraniteľnosti musia byť nahlásené ENISA do 24 hodín.
5. Zabezpečte poskytovanie bezpečnostných aktualizácií po dobu podpory produktu (minimálne 5 rokov alebo očakávaná doba používania).
6. Vypracujte technickú dokumentáciu a vyhlásenie o zhode – uchovávajte minimálne 10 rokov po uvedení produktu na trh.

8.3.3 Kroky pre súlad s NIS2

Pre prevádzkovateľov základnej služby:

1. Vykonajte sebaidentifikáciu – overte, či váš podnik spĺňa kritériá prevádzkovateľa základnej služby podľa zákona č. 366/2024 Z. z.
2. Zaregistrujte sa na NBÚ prostredníctvom portálu slovensko.sk (lehota 60 dní od vzniku povinnosti pre nové subjekty).
3. Vykonajte analýzu rizík podľa metodiky NBÚ (účinná od septembra 2025) – identifikujte aktíva, hrozby a zraniteľnosti.
4. Implementujte bezpečnostné opatrenia podľa § 20 zákona – pravidlo 3-2-1 pre zálohovanie, MFA pre kritické systémy, patch management, riadenie prístupov.
5. Vypracujte bezpečnostnú dokumentáciu – politiky, plán kontinuity podnikania (BCP), plán obnovy po havárii (DRP), plán reakcie na incidenty.
6. Vyškoľte zamestnancov – pravidelné školenia kybernetickej bezpečnosti pre všetkých zamestnancov.
7. Pripravte proces hlásenia incidentov – včasné varovanie do 24 hodín, oznámenie do 72 hodín, záverečná správa do 30 dní.

Tab. č. 43: **Checklist prioritných opatrení pre MSP**

Opatrenie	Relevantná regulácia	Priorita
Školenie AI gramotnosti zamestnancov	AI Act	**URGENTNÉ**
Inventarizácia AI systémov	AI Act	**VYSOKÁ**
Registrácia na NBÚ (ak sa týka)	NIS2	**VYSOKÁ**
Analýza rizík	NIS2	**VYSOKÁ**
Implementácia MFA	NIS2, všeobecná bezpečnosť	**VYSOKÁ**
Zálohovanie podľa pravidla 3-2-1	NIS2, CRA	**VYSOKÁ**
Vytvorenie SBOM (výrobcovia)	CRA	**STREDNÁ**
Certifikácia ISO 27001	NIS2, CRA (odporúčané)	**STREDNÁ**

Zdroj: Vlastné spracovanie

8.4 Využitie dostupných podporných nástrojov

EÚ a slovenské inštitúcie poskytujú MSP rozsiahlu podpornú infraštruktúru, ktorej nevyužitie predstavuje zbytočnú konkurenčnú nevýhodu. MSP by mali aktívne využívať tieto nástroje na zníženie nákladov compliance a získanie odborného poradenstva.

8.4.1 Európske centrá digitálnych inovácií (EDIH)

Na Slovensku pôsobí päť EDIH (HOPERO, CASSOVIUM, HealthHub, EXPANDI 4.0 a SCDI), ktoré poskytujú MSP bezplatné alebo dotované služby vrátane testovania technológií, školení, poradenstva a networkingu. Od roku 2025 EDIH fungujú aj ako AI helpdesky pre otázky súvisiace s AI Act.

Odporúčané využitie EDIH:

- Bezplatné konzultácie k regulačným požiadavkám
- Testovanie AI systémov a digitálnych produktov

- Školenia kybernetickej bezpečnosti a AI gramotnosti
- Pomoc pri získavaní financovania
- Prepojenie s potenciálnymi partnermi a zákazníkmi.

8.4.2 Regulačné sandboxy

AI Act vyžaduje, aby každý členský štát zriadil regulačný sandbox do augusta 2026. MSP vyvíjajúce inovatívne AI systémy by mali zvážiť účasť v sandboxe, ktorý poskytuje bezpečné prostredie pre vývoj a testovanie pod dohľadom regulátora, prioritný prístup pre MSP a startupy, ochranu pred pokutami počas účasti a dokumentáciu, ktorú možno použiť ako dôkaz súladu.

8.4.3 Finančná podpora

Dostupné zdroje financovania:

- Granty NCC-SK na kybernetickú bezpečnosť – podpora až do 90 % nákladov na vypracovanie bezpečnostnej dokumentácie
- Program Digitálna Európa – financovanie projektov v oblasti AI, kybernetickej bezpečnosti a digitálnych zručností
- Plán obnovy a odolnosti SR – prostriedky na digitálnu transformáciu a kybernetickú bezpečnosť
- Program Slovensko 2021–2027 – podpora inovácií a digitalizácie MSP
- Schéma de minimis – štátna pomoc pre MSP do 300 000 EUR počas troch rokov.

8.5 Budovanie interných kapacít

Dlhodobá konkurencieschopnosť MSP v novom regulačnom prostredí závisí od budovania interných kapacít. Závislosť výlučne na externých poskytovateľoch je nákladná a nespoľahlivá.

8.5.1 Vzdelávanie a rozvoj zamestnancov

Prioritné oblasti vzdelávania:

1. AI gramotnosť (povinná od februára 2025) – pochopenie fungovania AI, jej prínosov a rizík, správne používanie AI nástrojov
2. Kybernetická bezpečnosť pre všetkých – rozpoznávanie phishingu, bezpečnosť hesiel, práca s citlivými údajmi
3. Špecializované školenia pre IT personál – správa bezpečnostných systémov, reakcia na incidenty, penetračné testovanie
4. Compliance školenia pre manažment – prehľad regulačných požiadaviek, zodpovednosť vedenia, riadenie rizík.

8.5.2 Organizačné opatrenia

Odporúčané organizačné kroky:

- Určenie zodpovednej osoby za kybernetickú bezpečnosť a compliance – nemusí ísť o plný úväzok, ale musí byť jasná zodpovednosť

- Zapojenie vrcholového vedenia – NIS2 výslovne stanovuje zodpovednosť vedenia za kybernetickú bezpečnosť
- Vytvorenie dokumentácie – politiky, procedúry, plány reakcie na incidenty
- Pravidelné interné audity – overovanie účinnosti opatrení a identifikácia medzier.

8.5.3 Zváženie outsourcingu

Pre MSP bez dostatočných interných kapacít môže byť outsourcing určitých funkcií nákladovo efektívnejším riešením než budovanie vlastného tímu. Podľa analýzy môže outsourcing kybernetickej bezpečnosti priniesť úspory 35–60 % oproti internému riešeniu.

Vhodné oblasti pre outsourcing:

- Managed Security Services (MSSP) – monitoring 24/7, správa bezpečnostných zariadení
- Zdieľaný CISO/DPO – odborník zdieľaný medzi viacerými MSP
- Penetračné testovanie a bezpečnostné audity
- Právne poradenstvo pre compliance.

8.6 Monitoring regulačného vývoja a adaptácia

Regulačné prostredie nie je statické. Výklady regulácií sa vyvíjajú, Európska komisia vydáva usmernenia a kódexy praxe a na národnej úrovni sa prijímajú vykonávacie predpisy. MSP musia systematicky sledovať tento vývoj a byť pripravené na adaptáciu.

8.6.1 Zdroje informácií

Odporúčané zdroje pre sledovanie vývoja:

- Európska komisia – digital-strategy.ec.europa.eu pre AI Act a CRA
- NBÚ – nbu.gov.sk pre NIS2 a kybernetickú bezpečnosť
- MIRRI – mirri.gov.sk pre digitalizáciu a AI
- Slovak Business Agency – sbagency.sk pre podporu MSP
- EDIH – edihslovensko.sk pre praktické poradenstvo
- Odborné združenia – IT Asociácia Slovenska, SOPK.

8.6.2 Flexibilita a pripravenosť na zmeny

Odporúčania pre flexibilnú adaptáciu:

- Investovanie do škálovateľných riešení, ktoré možno upraviť bez kompletnej prestavby
- Budovanie modulárnych procesov compliance, nie monolitické štruktúry
- Udržiavanie kontaktu s regulátormi a odbornými komunitami
- Participácia na konzultačných procesoch – hlas MSP môže ovplyvniť budúce pravidlá
- Pravidelne prehodnocovanie compliance stratégie (minimálne ročne).

8.7 Záverečné zhrnutie odporúčaní

Technologické regulácie EÚ predstavujú pre slovenské MSP zásadnú zmenu podnikateľského prostredia. Nie je však dôvod na paniku – regulácie boli navrhované

s ohľadom na potreby MSP a obsahujú mechanizmy na zmiernenie záťaže. Kľúčom k úspechu je proaktívny, informovaný a strategický prístup.

Desať kľúčových odporúčaní pre MSP:

1. Nepodceňovať regulácie – aj keď sa niektoré regulácie nemusia týkať konkrétneho MSP, môžu ho ovplyvniť cez dodávateľský reťazec alebo očakávania zákazníkov
2. Začať so sebahodnotením – je potrebné identifikovať, ktoré regulácie a v akom rozsahu sa na konkrétne MSP vzťahujú
3. Voľba explicitnej stratégiu – líder, nasledovník, adaptér alebo exiter
4. Využívanie podporných nástrojov – EDIH, granty, sandboxy sú dostupné pre MSP
5. Priorizovanie opatrení – je potrebné začať od najurgentnejších (AI gramotnosť, registrácia NBÚ)
6. Investovanie do ľudí/zamestnancov – vzdelávanie zamestnancov je najlepšia investícia
7. Budovanie bezpečnostnej kultúry – nielen technológie, ale aj procesy a povedomie sú dôležité
8. Komunikacia "compliance" – je vhodné ho používať ako konkurenčnú výhodu voči zákazníkom
9. Sledovanie vývoja – regulačné prostredie sa mení, je vhodné a odporúčané aby MSP zostali informovaní
10. Proaktivita – reaktívny prístup je vždy drahší a riskantnejší

MSP, ktoré pochopia novú regulačnú realitu, strategicky na ňu zareagujú a využijú dostupnú podporu, môžu z tejto zmeny vyjsť posilnené. Tie, ktoré ju budú ignorovať alebo vnímať len ako záťaž, riskujú dlhodobú stratu konkurencieschopnosti. Rozhodnutie je na každom podniku – a čas na jeho prijatie je teraz.

ZÁVER

Táto analýza zhodnotila dopady troch kľúčových technologických regulácií Európskej únie – AI Act, Cyber Resilience Act (CRA) a smernice NIS2 – na konkurencieschopnosť malých a stredných podnikov na Slovensku. Regulácie predstavujú štrukturálnu zmenu podnikateľského prostredia, ktorá presahuje rámec sektorových úprav a zásadne redefinuje podmienky fungovania digitálnej ekonomiky.

Kľúčové zistenia

Technologické regulácie EÚ vytvárajú nový normatívny rámec, v ktorom sa digitálna bezpečnosť, transparentnosť a zodpovednosť stávajú povinným štandardom. Ich kumulatívny efekt znamená, že compliance už nie je okrajovou právnou otázkou, ale integrálnou súčasťou podnikateľskej stratégie.

Náklady na dosiahnutie súladu sa v prípade MSP pohybujú približne v rozsahu 0,8 – 1,9 % ročného obratu, pričom ich regresívny charakter znamená vyššiu proporcionálnu záťaž pre mikropodniky a malé podniky. Hoci tieto náklady nie sú zanedbateľné, sú makroekonomicky zvládnuteľné a je potrebné ich hodnotiť v kontexte prínosov – harmonizovaného prístupu na jednotný trh EÚ, vyššej dôvery zákazníkov, zníženia rizika kybernetických incidentov a posilnenia postavenia v dodávateľských reťazcoch.

Dopad na inovácie má duálny charakter. Krátkodobo môže dôjsť k presunu zdrojov z výskumu a vývoja do compliance aktivít a k zvýšeniu bariér vstupu na trh. Dlhodobo však harmonizovaný regulačný rámec, regulačné sandboxy, podpora prostredníctvom EDIH a rastúci dopyt po bezpečných riešeniach vytvárajú predpoklady pre vznik nových trhových príležitostí. Výsledný efekt závisí od miery adaptability podnikov a kvality implementácie regulačných mechanizmov. Osobitný význam nadobúdajú dodávateľské reťazce, prostredníctvom ktorých sa regulačné požiadavky prenášajú aj na podniky, ktoré nie sú priamo regulovanými subjektmi. Compliance sa tak stáva faktickou podmienkou prístupu na trh, najmä pri spolupráci s veľkými podnikmi a subjektmi verejnej správy.

Strategické implikácie pre MSP a verejnú politiku

Pre malé a stredné podniky predstavujú regulácie nielen povinnosť, ale aj strategické rozhodnutie. Podniky, ktoré pristúpia k reguláciám reaktívne a budú ich vnímať výlučne ako náklad, riskujú postupnú stratu konkurencieschopnosti. Naopak, podniky, ktoré integrujú compliance do svojho biznis modelu, môžu využiť regulačnú zmenu ako nástroj diferenciácie a budovania dôvery.

Na strane štátu je kľúčová proporcionalita a predvídateľnosť dohľadu, zjednodušenie metodických usmernení, cielené finančné nástroje reflektujúce regresívny charakter nákladov a systematická podpora budovania digitálnych a kybernetických kapacít MSP. Slovensko disponuje funkčnou podpornou infraštruktúrou (EDIH, NCC-SK, SBA a ďalšie inštitúcie), avšak jej efektívna koordinácia a dostupnosť pre najmenšie podniky zostáva výzvou.

Perspektíva ďalšieho vývoja

Technologické regulácie EÚ sú súčasťou širšieho procesu konsolidácie digitálneho regulačného rámca. Očakáva sa ďalšia harmonizácia a zjednodušovanie pravidiel, ako aj postupné prenášanie európskych štandardov do globálneho prostredia. Pre slovenské MSP to znamená, že investície do súladu s európskymi normami môžu predstavovať dlhodobú konkurenčnú výhodu aj mimo trhu EÚ. Súčasne rastúca sofistikovanosť kybernetických hrozieb potvrdzuje, že bezpečnosť už nie je doplnkovou funkciou, ale základnou podnikateľskou kompetenciou. MSP, ktoré túto realitu akceptujú a systematicky budujú svoju digitálnu odolnosť, budú lepšie pripravené na budúce riziká aj príležitosti.

Záverečné konštatovanie

Technologické regulácie EÚ nepredstavujú len administratívnu povinnosť, ale systémovú transformáciu digitálneho hospodárstva. Ich dopady na slovenské MSP sú významné, no nie neprekonateľné. Kľúčovým faktorom úspechu bude schopnosť podnikov pristúpiť k reguláciám strategicky, využiť dostupnú podporu a premeniť compliance z nákladovej položky na prvok konkurenčnej výhody. Voľba medzi pasívnou adaptáciou a aktívnym využitím regulačnej zmeny bude rozhodujúcim faktorom budúcej konkurencieschopnosti slovenských MSP.

Zoznam použitých zdrojov

A-LIGN. (2024). 2024 Compliance Benchmark Report. Tampa, FL: A-LIGN.

Blind, K., Niebel, T., Ramel, F., & Ziesemer, T. (2023). The impact of the General Data Protection Regulation (GDPR) on innovation: Evidence from the German innovation survey. Industry and Innovation, 30(8), 1002–1026.

Bradford, A. (2012). The Brussels Effect. Northwestern University Law Review, 107(1), 1–67.

Corbett, J., Lehtonen, J., Pearson, S., et al. (2021). The impact and effectiveness of Innovate UK and FCA regulatory sandboxes. London: Financial Conduct Authority.

EDIH Slovensko. (n.d.). Európske digitálne inovačné huby. Dostupné na internete: https://www.edihslovensko.sk

ENISA. (2024). NIS Investments 2024 Report. Dostupné na internete: https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf

European Central Bank. (2024). Survey on the Access to Finance of Enterprises (SAFE).

European Commission. (2022). Impact assessment report accompanying the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act) (SWD(2022)).

European Commission. (2023). Annual burden survey 2022: Regulatory costs and administrative burden for SMEs.

European Commission. (2023). Flash Eurobarometer 531 – SMEs, cross-border trade and regulatory barriers.

European Commission. (2024). European Digital Innovation Hubs (EDIH) Network Report 2023.

European Commission. (2024). Regulation (EU) 2024/1689 – Artificial Intelligence Act.

European Commission. (2024). Special Eurobarometer 554 – Artificial Intelligence and the future of digital technologies.

European Commission. (n.d.). Proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act).

European Parliament. (2024). The impact of EU legislation on SMEs – Costs and benefits. Luxembourg: Publications Office of the European Union.

Frontier Economics. (2022). The economic impact of the NIS2 Directive.

Gartner. (2023). Predicts 2023: Cybersecurity – SBOMs become foundational to software supply chain security. Stamford, CT: Gartner.

IBM Security. (2024). Cost of a data breach report 2024. Armonk, NY: IBM Corporation. Dostupné na internete: https://www.ibm.com/reports/data-breach

Intellera Consulting. (2022). The economic impact of the Artificial Intelligence Act on European SMEs.

International Organization for Standardization. (2023). ISO survey of management system standard certifications 2023.

ISC. (2023). Cybersecurity workforce study 2023.

ISMS.online. (2024). NIS 2 compliance costs: Overview of compliance investments and hidden fees. Dostupné na internete: https://www.isms.online/nis-2/overview/costs/

Jia, J., Jin, G. Z., & Wagman, L. (2019). The short-run effects of GDPR on technology venture investment. CEPR Discussion Paper.

Jia, J., Jin, G. Z., & Wagman, L. (2021). The short-run effects of the General Data Protection Regulation on technology venture investment. Marketing Science, 40(4), 662–684.

LinkedIn Corporation. (2024). Workplace Learning Report 2024.

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR. (2024). Digitálne zručnosti na Slovensku: Najaktuálnejšie dáta ukazujú, kde napredujeme a kde zaostávame. Dostupné na internete: https://digitalnabuducnost.gov.sk/digitalne-zrucnosti-na-slovensku-najaktualnejsie-data-ukazuju-kde-napredujeme-a-kde-zaostavame/

Ministerstvo investícií, regionálneho rozvoja a informatizácie SR. (n.d.). Dostupné na: https://mirri.gov.sk/

MIT Sloan. (2024). GDPR reduced firms' data and computation use. Dostupné na internete: https://mitsloan.mit.edu/ideas-made-to-matter/gdpr-reduced-firms-data-and-computation-use

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)

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

Nariadenie Európskeho parlamentu a Rady (EÚ) 2024/2847 z 23. októbra 2024 o horizontálnych požiadavkách kybernetickej bezpečnosti pre produkty s digitálnymi prvkami a o zmene nariadení (EÚ) č. 168/2013 a (EÚ) 2019/1020 a smernice (EÚ) 2020/1828 (akt o kybernetickej odolnosti)

Národný bezpečnostný úrad. (2025). Metodika analýzy rizík kybernetickej bezpečnosti (verzia 2.0). Dostupné na internete: https://www.nbu.gov.sk/data/att/3446.pdf

National Institute of Standards and Technology. (2021). Apache Log4j2 remote code execution vulnerability.

Odporúčanie Komisie (EÚ) č. 2025/1099 z 21. mája 2025 o definícii malých podnikov so strednou trhovou kapitalizáciou

Odporúčanie Komisie č. 2003/361/ES zo 6. mája 2003, ktoré sa týka definície mikro, malých a stredných podnikov

Payscale. (2024). Cyber security salary in Belgium. Dostupné na internete: https://www.payscale.com/research/BE/Skill%3DCyber_Security/Salary

Ponemon Institute. (2024). Cost of a data breach report 2024.

Porter, M. E., & van der Linde, C. (1995). Toward a new conception of the environment–competitiveness relationship. Journal of Economic Perspectives, 9(4), 97–118.

PwC. (2024). Global Digital Trust Insights 2024.

Renda, A., Schrefler, L., Bontoux, L., et al. (2021). Study to support an impact assessment of regulatory requirements for artificial intelligence in Europe. CEPS.

Smernica (EÚ) 2022/2555 Európskeho parlamentu a Rady zo 14. decembra 2022 o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2). Úradný vestník Európskej únie.

U.S. Cybersecurity and Infrastructure Security Agency. (2020). Advanced persistent threat compromise (SolarWinds).

Verizon. (2024). Data breach investigations report 2024.

Zákon č. 366/2024 Z. z. z 28. novembra 2024, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony.

Zákon č. 69/2018 Z. z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov