SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

V PRAZE DNE 15. ČERVENCE 2026

Stanovisko Svazu průmyslu a dopravy ČR k návrhu nařízení Cloud and AI Development Act (CADA)

I. Obecné stanovisko

Svaz průmyslu a dopravy ČR (SP ČR) podporuje cíl Evropské komise posílit evropskou digitální suverenitu, bezpečnost a odolnost cloudových služeb a vytvořit důvěryhodný rámec pro širší využívání cloud computingu a umělé inteligence ve veřejném sektoru. Posilování evropských technologických kapacit, rozvoj evropské cloudové infrastruktury a snižování strategických závislostí představují legitimní cíle, které mohou přispět ke zvýšení konkurenceschopnosti, bezpečnosti i technologické odolnosti Evropské unie.

Současně se však SP ČR domnívá, že návrh CADA ve své současné podobě vyžaduje významné dopracování. Návrh zavádí nový horizontální regulatorní rámec s dopady na veřejnou správu, provozovatele kritické infrastruktury i soukromý sektor, aniž by dostatečně prokazoval, že navržená opatření představují nejúčinnější a nejproporcionálnější způsob dosažení deklarovaných cílů.

Chybí komplexní posouzení dopadů návrhu

SP ČR postrádá podrobnější analýzu ekonomických, technologických a tržních dopadů návrhu. Z předložené dokumentace není dostatečně zřejmé, jaký bude dopad navrhovaných požadavků na hospodářskou soutěž, investice do evropské cloudové infrastruktury, náklady veřejného sektoru, dostupnost cloudových služeb ani tempo digitální transformace členských států.

Současně není doloženo, že po vstupu nařízení v platnost bude na trhu existovat dostatečný počet poskytovatelů schopných splnit požadavky jednotlivých úrovní Union Assurance Levels (UAL). Návrh rovněž nehodnotí dopady na již realizované investice veřejné správy ani náklady spojené s případnou migrací existujících cloudových řešení.

Vzhledem k rozsahu navrhované regulace považuje SP ČR doplnění komplexní dopadové analýzy za nezbytný předpoklad dalšího projednávání návrhu.

Digitální suverenita by měla být založena na řízení rizik

SP ČR podporuje posilování evropské digitální suverenity. Domníváme se však, že digitální suverenita by měla být posuzována především podle skutečné úrovně bezpečnosti, provozní odolnosti a kontroly nad daty.

TELEFON (+420) 731 829 128 | E-MAIL SPCR@SPCR.CZ
WEB WWW.SPCR.CZ | ADRESA FREYOVA 948/11, 190 00 PRAHA 9
ZAPSANÝ VE SPOLKOVÉM REJSTŘÍKU, VEDENÉM MĚSTSKÝM SOUDEM V PRAZE ODDÍL L, VLOŽKA 3148.
IČO: 00536211, DIČ: CZ00536211.

Významnými kritérii by měla být zejména technická a organizační bezpečnostní opatření, šifrování, správa kryptografických klíčů, řízení přístupových oprávnění, auditovatelnost, možnost bezpečné migrace mezi poskytovateli, odolnost vůči kybernetickým incidentům a schopnost zajistit kontinuitu poskytovaných služeb.

SP ČR proto podporuje regulatorní rámec založený na řízení rizik, technologické neutralitě a objektivně ověřitelných bezpečnostních požadavcích. Posouzení rizik by však mělo zohledňovat všechny relevantní okolnosti, včetně případných rizik vyplývajících z jurisdikce poskytovatele, přístupu orgánů třetích zemí k datům nebo vzniku strategických závislostí v nejcitlivějších případech použití.

Návrh musí lépe zohlednit fungování cloudového ekosystému

Cloudové služby dnes nepředstavují izolované produkty jednotlivých poskytovatelů, ale komplexní technologický ekosystém tvořený infrastrukturou, platformami, databázovými službami, bezpečnostními nástroji, AI službami, open-source komponenty i rozsáhlými dodavatelskými řetězci.

Regulatorní požadavky se proto nedotknou pouze poskytovatelů cloudových služeb, ale celého evropského digitálního ekosystému včetně poskytovatelů SaaS řešení, systémových integrátorů, evropských technologických společností, startupů, provozovatelů kritické infrastruktury i veřejného sektoru.

SP ČR se domnívá, že návrh tuto skutečnost dostatečně nezohledňuje. Zejména není zřejmé, jak budou jednotlivé požadavky aplikovány na celý cloudový stack ani jak budou posuzovány jednotlivé komponenty a subdodavatelské vztahy. Bez tohoto vyjasnění může docházet k rozdílnému výkladu jednotlivých ustanovení a významné právní nejistotě.

Současně považujeme za důležité, aby regulace jasně rozlišovala mezi cloudovou infrastrukturou, platformními službami, aplikační vrstvou, průmyslovými SaaS řešeními a AI službami. Automatické přenášení požadavků určených primárně pro cloudovou infrastrukturu na aplikační vrstvu nebo zakázková průmyslová SaaS řešení by mohla nepřiměřeně zvýšit regulatorní náklady a negativně ovlivnit investice do průmyslové umělé inteligence, datově řízených služeb a digitální transformace evropského průmyslu.

Klíčovým aspektem digitální suverenity a autonomie evropských podniků i veřejné správy je taky účinná ochrana před uzamčením u jednoho poskytovatele (vendor lock-in). SP ČR proto doporučuje, aby CADA aktivně řešil protisoutěžní praktiky v oblasti softwarových licencí. Nařízení by mělo explicitně zakotvit plnou přenositelnost licencí (licensing portability) mezi poskytovateli, nařídit nediskriminační naceňování softwarových licencí a garantovat softwarovou i bezpečnostní ekvivalenci bez ohledu na zvolenou cloudovou platformu. Bez možnosti volného pohybu mezi cloudy nelze skutečné suverenity ani technologické odolnosti dosáhnout.

CADA musí být konzistentní se stávající evropskou legislativou

SP ČR považuje za nezbytné, aby CADA byl plně provázán se stávajícím evropským regulatorním rámcem, zejména s AI Act, směrnicí NIS2, s revizí Aktu o kybernetické bezpečnosti (CSA2), s nařízením DORA, Cyber Resilience Act a dalšími sektorovými předpisy.

Nový regulatorní rámec by měl stávající pravidla doplňovat, nikoli vytvářet nové překrývající se nebo duplicitní povinnosti. V opačném případě hrozí zvýšení regulatorní zátěže bez odpovídajícího přínosu pro bezpečnost nebo odolnost digitální infrastruktury.

Urychlení rozvoje infrastruktury a udržitelná digitální transformace

SP ČR zdůrazňuje, že rozvoj cloudových a AI služeb v Evropě kriticky závisí na rychlosti výstavby fyzické datové infrastruktury. Současné povolovací procesy pro datová centra v členských státech trvají často 5 až 7 let kvůli složitým plánovacím pravidlům. CADA by měl aktivně podpořit zkrácení těchto lhůt prostřednictvím mechanismů předběžného přezkumu (pre-permit review), digitalizace procesů a omezení námitek během územního řízení pouze na bezprostřední sousedy.

Vítáme záměr využít status „zvláštního projektu" pro zjednodušení povolování a přístupu k síti. Tyto výhody by však měly být dostupné pro všechny životaschopné projekty, i mimo určené akcelerační zóny. V oblasti udržitelnosti doporučujeme sladit národní kritéria s připravovaným celounijním systémem hodnocení a zajistit, aby tato pravidla nepenalizovala nejefektivnější technologie chlazení, jako je chlazení vodou (water cooling). CADA by měl rovněž usnadnit plánování rozvodných sítí, flexibilní smlouvy o připojení a širší využívání smluv o nákupu elektřiny z obnovitelných zdrojů (PPA).

Obecný závěr

SP ČR je přesvědčen, že návrh CADA představuje důležitou iniciativu pro další rozvoj evropského cloudového trhu. Aby však mohl naplnit své cíle, je nezbytné návrh dále dopracovat. Budoucí regulatorní rámec by měl být založen na objektivním posouzení rizik, technologické neutralitě, právní jistotě, proporcionalitě jednotlivých požadavků a respektování stávající evropské legislativy. Současně by měl podporovat bezpečnost a odolnost cloudových služeb, aniž by nepřiměřeně omezoval hospodářskou soutěž, inovace nebo digitální transformaci veřejného sektoru.

II. Konkrétní připomínky k návrhu

2.1 Článek 17 – Uznávání Union Assurance Levels

SP ČR podporuje vytvoření jednotného evropského systému certifikace cloudových služeb, který přispěje k vyšší důvěře veřejného sektoru při jejich využívání a současně omezí rozdílné přístupy jednotlivých členských států. Současně se však domníváme, že navržený mechanismus uznávání jednotlivých úrovní Union Assurance Levels vyžaduje další zpřesnění.

Návrh v současné podobě dostatečně nevymezuje kritéria, podle kterých budou jednotlivé úrovně UAL posuzovány, ani vztah mezi národními certifikačními orgány, ostatními členskými státy a Evropskou komisí. Výsledný proces by proto mohl vést k rozdílnému výkladu certifikačních požadavků, prodlužování certifikačních řízení a regulatorní nejistotě pro poskytovatele cloudových služeb i jejich zákazníky.

SP ČR považuje za nezbytné, aby rozhodování o přiznání jednotlivých úrovní UAL bylo založeno především na transparentních, objektivních a technicky ověřitelných kritériích. Současně jednoznačně doporučujeme vymezit kompetence jednotlivých subjektů zapojených do certifikačního procesu, včetně pravidel pro řešení případných rozdílných stanovisek mezi členskými státy.

Zároveň je vhodné jasně vymezit, zda se posuzování vztahuje na celou službu, konkrétní komponentu, datovou lokalitu, subdodavatele nebo konkrétní způsob využití služby. Bez takového rozlišení může být pro poskytovatele i zákazníky obtížné posoudit dopady na stávající cloudová řešení, dodavatelské řetězce a případné úpravy poskytovaných služeb.

Návrh by měl rovněž zajistit dostatečnou ochranu obchodního tajemství a důvěrných technických informací předkládaných v rámci certifikace. Rozsah požadovaných informací by měl být vždy přiměřený sledovanému účelu a neměl by vést k nepřiměřenému zpřístupňování citlivé technické dokumentace nebo zdrojového kódu. Certifikační a auditní proces by současně neměl vyžadovat zpřístupňování detailů bezpečnostní architektury, informací o dodavatelském řetězci, datových tocích nebo jiných citlivých technických informací nad rámec toho, co je nezbytné k ověření splnění požadovaných bezpečnostních kritérií. Ochrana obchodního tajemství a důvěrných informací by měla být v rámci systému UAL výslovně zakotvena jako jeden ze základních principů certifikačního procesu.

Dále SP ČR upozorňuje na rizika spojená s požadavky na lokalizaci dat u nižších úrovní zabezpečení (UAL 1 a UAL 2). Požadavek na uchovávání veškeré telemetrie a vzorců kybernetických hrozeb výhradně v Evropě (Annex II, sekce 1.1c) může paradoxně oslabit evropskou bezpečnost, neboť znemožní globální sdílení informací o hrozbách v reálném čase. Navrhujeme proto odstranit lokalizační požadavky na metadata a telemetrii pro úrovně UAL 1 a UAL 2.

U nejvyšších úrovní (UAL 3 a UAL 4) považujeme navržená kritéria za extrémní, neboť jdou nad rámec i těch nejpřísnějších národních standardů členských států a de facto vylučují důvěryhodné globální partnery z podpory klíčových obranných či citlivých služeb.

2.2 Článek 18 – Uznávání třetích zemí

SP ČR vítá zavedení mechanismu umožňujícího uznávání ekvivalentních bezpečnostních rámců třetích zemí. Zachování možnosti uznat srovnatelnou úroveň bezpečnosti představuje důležitý předpoklad pro fungování otevřeného a konkurenceschopného evropského cloudového trhu.

Současně se domníváme, že podmínky tohoto mechanismu vyžadují další dopracování. Navržená kritéria jsou nastavena kumulativně a jejich proporcionalita není dostatečně odůvodněna. V praxi tak může docházet k situacím, kdy nebude možné uznat služby, které objektivně splňují požadovanou úroveň bezpečnosti a provozní odolnosti.

SP ČR proto doporučuje, aby mechanismus ekvivalence vycházel především z objektivního posouzení skutečně dosažené úrovně bezpečnosti, technických a organizačních opatření, provozní odolnosti a schopnosti zajistit ochranu dat. Kritéria by měla být předvídatelná, transparentní a technologicky neutrální.

Současně doporučujeme zvážit možnost využití mechanismu ekvivalence i pro vyšší úrovně UAL, pokud budou splněny všechny bezpečnostní požadavky stanovené tímto nařízením.

2.3 Článek 29 – Posuzování rizik

SP ČR považuje článek 29 za jedno z klíčových ustanovení návrhu, neboť určuje způsob posuzování rizik i rozdělení odpovědností mezi členskými státy a Evropskou komisí. Právě na základě tohoto ustanovení budou veřejné instituce určovat požadovanou úroveň Union Assurance Levels pro jednotlivé činnosti a informační systémy.

SP ČR podporuje přístup založený na řízení rizik. Domníváme se, že skutečná úroveň rizika představuje nejvhodnější základ pro určování požadované úrovně zabezpečení cloudových služeb. Současně však návrh ponechává řadu nejasností, které mohou vést k rozdílnému výkladu i aplikační praxi.

Především není dostatečně zřejmé, jaký bude vztah mezi národním hodnocením rizik, rozhodnutím příslušného certifikačního orgánu a případným přezkumem ze strany Evropské komise. Návrh by měl jednoznačně vymezit odpovědnosti jednotlivých subjektů i postup při řešení rozdílných závěrů. Současná úprava neposkytuje dostatečnou právní jistotu veřejným zadavatelům ani poskytovatelům cloudových služeb.

Stejně tak by měly být jasně vymezeny podmínky, za nichž může Evropská komise prostřednictvím delegovaných či prováděcích aktů rozšiřovat požadované úrovně UAL nebo ukládat dodatečná opatření. Takové zásahy by měly být řádně odůvodněny, transparentní, předvídatelné a měly by vznikat po konzultaci s členskými státy a dotčenými stakeholdery.

SP ČR současně upozorňuje, že posuzování rizik v oblastech souvisejících s národní bezpečností, veřejným pořádkem nebo ochranou kritické infrastruktury představuje odpovědnost členských států. Návrh by měl zachovat koordinační úlohu Evropské komise, neměl by však vytvářet mechanismus, který by fakticky umožňoval nahrazovat bezpečnostní hodnocení provedené členskými státy. V této souvislosti doporučujeme znovu posoudit navržené rozdělení kompetencí s ohledem na primární právo Evropské unie, zejména článek 72 SFEU.

Za problematickou považujeme rovněž navrženou dvanáctiměsíční lhůtu pro migraci na vyšší úroveň Union Assurance Levels. U rozsáhlých cloudových implementací veřejné správy nebo provozovatelů kritické infrastruktury se jedná o lhůtu, která zpravidla nebude odpovídat technické ani smluvní realitě. Z konzultací s členskými společnostmi vyplývá, že přizpůsobení infrastruktury požadavkům vyšších úrovní UAL může v závislosti na rozsahu služeb vyžadovat jeden až tři roky. Návrh by proto měl umožnit přiměřenější implementační období nebo individuální posouzení podle rozsahu konkrétní migrace. Při stanovování migračních požadavků je současně nezbytné zohlednit nejen technickou realizovatelnost, ale také smluvní závazky, kontinuitu poskytovaných služeb, požadavky kybernetické bezpečnosti a provozní rizika spojená se změnou poskytovatele. U rozsáhlých implementací by proto mělo být možné využít individuální migrační plán, přiměřené přechodné období nebo odůvodněné výjimky v případech, kdy by okamžitá migrace mohla ohrozit kontinuitu služeb nebo bezpečnost kritické infrastruktury.

Stanovení požadovaných úrovní UAL by nemělo vytvářet obecné zmocnění Evropské komise ukládat závazné požadavky na využívání konkrétních cloudových řešení jednotlivým odvětvím soukromého sektoru nad rámec výslovně stanovený v nařízení.

2.4 Článek 30 – Výjimky

SP ČR vítá zachování mechanismu umožňujícího využití cloudových služeb mimo systém Union Assurance Levels v mimořádných situacích nebo v případech, kdy na trhu není dostupné řešení splňující požadovanou úroveň zabezpečení. Takový mechanismus představuje důležitou pojistku pro zajištění kontinuity veřejných služeb.

Současně doporučujeme přesněji vymezit podmínky využívání těchto výjimek. Pravidla by měla být dostatečně jasná a jednotná, aby veřejní zadavatelé měli právní jistotu při jejich aplikaci a aby nedocházelo k rozdílnému výkladu mezi členskými státy.

2.5 Článek 31 – Kritické sektory a vztah k další evropské legislativě

SP ČR považuje za nezbytné zajistit plnou provázanost CADA se stávající evropskou digitální legislativou. Většina subjektů, na které bude návrh dopadat, již dnes plní rozsáhlé regulatorní povinnosti podle AI Act, směrnice NIS2, nařízení DORA a dalších sektorových předpisů.

Současný návrh dostatečně nevysvětluje, jak budou jednotlivé regulatorní režimy vzájemně provázány. Není například zřejmé, jak budou rozděleny odpovědnosti mezi poskytovatele cloudové služby, poskytovatele AI systému a provozovatele kritické infrastruktury ani jak budou v praxi aplikovány jednotlivé povinnosti v oblasti řízení rizik, testování, vedení záznamů, lidského dohledu nebo oznamování incidentů.

Bez jednoznačného vymezení těchto vztahů hrozí vznik duplicitních nebo překrývajících se regulatorních povinností, které zvýší administrativní zátěž, aniž by odpovídajícím způsobem přispěly ke zvýšení bezpečnosti.

SP ČR proto doporučuje doplnit návrh buď o explicitnější vymezení vztahu CADA k ostatním evropským právním předpisům, nebo o zmocnění Evropské komise vydat metodické pokyny obsahující praktické scénáře implementace pro jednotlivé sektory, zejména energetiku, dopravu, zdravotnictví a finanční sektor.

Tyto pokyny by měly podrobněji vyjasnit role a odpovědnosti jednotlivých aktérů, včetně poskytovatelů cloudových služeb, poskytovatelů AI systémů, systémových integrátorů a provozovatelů kritické infrastruktury. Současně by měly přispět k předcházení duplicitám v oblasti řízení rizik, oznamování incidentů, technické dokumentace, auditovatelnosti a testování, aby CADA nepřinášel další vrstvu regulatorních povinností bez odpovídající přidané hodnoty pro bezpečnost a odolnost digitální infrastruktury.