Digital Council

Pozice Digital Council ke Cloud and AI Development Act

Digital Council

Úvod

Digital Council podporuje základní ambici návrhu Cloud and AI Development Act (CADA). Evropa potřebuje více výpočetní kapacity, rychlejší a předvídatelnější povolování datových center, konkurenceschopnější cloudový ekosystém a důvěryhodný rámec pro ochranu kritických veřejných služeb a citlivých agend státu.

Evropská komise předložila návrh CADA dne 3. června 2026. Návrh se nachází na začátku řádného legislativního postupu; k rozhodnému datu Evropský parlament ani Rada nepřijaly svou vyjednávací pozici.[1]

Kapacitní a inovační část návrhu jde převážně správným směrem. Digital Council podporuje zejména části návrhu týkající se akceleračních zón pro datová centra, jednotných informačních míst, předvídatelnějšího povolování a možnosti označit některé plánované projekty datových center za strategické. Tato opatření mohou odstranit část překážek, které dnes brzdí investice do evropských datových center. Úspěch však bude záviset především na dostupnosti elektřiny, kapacitě energetických sítí, transparentních pravidlech připojení a přístupu podniků a výzkumných institucí k nově vytvořené výpočetní kapacitě.

Významnější změny vyžaduje navrhovaný rámec čtyř úrovní cloudové suverenity. Přísné požadavky jsou legitimní pro obranu, vnitřní bezpečnost, justici a další skutečně kritické činnosti. Neměly by se však automaticky vztahovat na běžné administrativní a podpůrné systémy veřejné správy.

Návrh vyžaduje, aby také nekritické veřejné činnosti používaly cloudové služby uznané alespoň na úrovni 1. Její podmínky přitom zahrnují evropské umístění infrastruktury a výlučné uchovávání zákaznických dat, metadat a telemetrie v EU, pokud veřejný zákazník výslovně nestanoví jinak.[2] Digital Council považuje evropskou datovou rezidenci zákaznických dat u úrovně 1 za legitimní nástroj podpory evropského cloudového a AI ekosystému, investic a transferu know-how. Takové pravidlo však nemá být automaticky a bez dalšího rozšiřováno na všechna metadata, telemetrii a provozní údaje bez rozlišení jejich citlivosti, technické funkce a bezpečnostního účelu.

Závažným implementačním rizikem je rovněž maximálně dvanáctiměsíční lhůta pro migraci, pokud posouzení rizik vyvolá potřebu změnit cloudovou službu. U složitých veřejných systémů může být nutné uskutečnit nové zadávací řízení, upravit integrace, převést data, otestovat bezpečnost a zajistit souběžný provoz. Univerzální roční limit proto může ohrozit kontinuitu právě těch služeb, které má návrh chránit.[3]

Digital Council prosazuje **otevřenou technologickou suverenitu** založenou na schopnosti volby, kontrole nad daty, interoperabilitě, bezpečnosti, provozní kontinuitě a možnosti změnit dodavatele. Evropa má rozvíjet vlastní technologie a kapacity, ale nemá se izolovat od důvěryhodných mezinárodních partnerů ani omezovat přístup k nejlepším dostupným řešením bez konkrétního a doloženého rizika.

Digital Council proto podporuje strategický směr CADA, ale doporučuje zásadně zpřesnit proporcionalitu rámce suverenity, upravit pojetí úrovně 1, prodloužit migrační období, respektovat odpovědnost členských států za národní bezpečnost, zabránit fragmentaci vnitřního trhu, omezit rozšiřování povinností prostřednictvím sekundární legislativy a zajistit skutečné vzájemné uznávání auditů.

Digital Council

Prioritní doporučení Digital Council

1. Rozlišovat mezi běžnými a skutečně kritickými agendami

Vyšší úrovně suverenity mají být vyžadovány pouze u konkrétních služeb a pracovních zátěží, jejichž narušení nebo zpřístupnění by mohlo vážně ohrozit bezpečnost, veřejný pořádek nebo kontinuitu základních funkcí státu.

2. Upravit úroveň 1 jako otevřený evropský standard

Úroveň 1 má stát zejména na kybernetické bezpečnosti, transparentnosti, přenositelnosti, řízení přístupu, kontrole zákazníka a evropské datové rezidenci zákaznických dat. Výlučná lokalizace všech metadat, telemetrie a provozních údajů v EU však nemá být automatickým pravidlem pro všechny běžné veřejné systémy bez rozlišení jejich citlivosti a technické funkce.

3. Uznávat rovnocenné technické, organizační a právní záruky

Šifrování, zákazníkem spravované klíče, oddělené evropské řízení služby, kontrolovaný vzdálený přístup, transparentní subdodavatelský řetězec a nezávislý audit mohou v řadě případů poskytovat účinnější ochranu než samotné geografické, vlastnické nebo formálně jurisdikční kritérium.

Exteritoriální právní rizika je nutné brát vážně. Nemají však být řešena pouze přes sídlo, původ kapitálu nebo vlastnickou strukturu. Rozhodující má být efektivní kontrola zákazníka nad daty, klíči, přístupy, provozem, auditem a právními zárukami.

4. Prodloužit migrační období

Základní období má činit nejméně 24 měsíců. Pro kritické nebo technicky složité systémy musí být možné schválit harmonogram v délce nejméně 36 měsíců nebo delší individuální harmonogram zohledňující zadávání zakázky, testování, bezpečnost a kontinuitu služby.

www.digitalcouncil.eu
prague@digitalcouncil.eu

Digital Council, z.ú.
Arbesovo náměstí 257/7, 150 00 Praha 5
IČO: 240 08 389

5. Respektovat odpovědnost členských států za národní bezpečnost

Společná evropská metodika je potřebná. Může být doplněna typovým katalogem veřejných služeb a pracovních zátěží, aby se omezila fragmentace vnitřního trhu. Pravomoc Komise změnit úroveň stanovenou členským státem však musí být výjimečná, přesně vymezená a doprovázená procesními zárukami. U záležitostí spadajících do národní bezpečnosti má mít Komise primárně metodickou a koordinační roli.

6. Nerozšiřovat povinnosti na soukromý sektor neurčitě prostřednictvím sekundární legislativy

Případné povinnosti pro energetiku, dopravu, zdravotnictví, bankovnictví nebo digitální infrastrukturu mohou být legitimní, pokud jde o skutečně kritickou infrastrukturu. Musí však být jasně vymezeny přímo v legislativním textu, podloženy posouzením dopadů a sladěny s NIS2, DORA a sektorovými pravidly.

7. Zavést princip „one audit – many uses“

Audity a důkazy předložené podle CADA, evropských certifikačních režimů a národních cloudových rámců se mají vzájemně uznávat. Duplicitní posouzení mají být přípustná pouze tam, kde řeší konkrétní dodatečné riziko.

8. Podporovat evropskou přidanou hodnotu bez uzavírání trhu

Kritéria veřejných zakázek mají oceňovat evropský výzkum, inovace, pracovní místa, interoperabilitu, bezpečnost dodávek a zapojení SME. Samotné sídlo, původ kapitálu nebo formální vlastnická struktura nejsou dostatečnými ukazateli skutečného přínosu pro Evropu.

Digital Council

1. Proč je CADA potřeba

Cloudové služby, datová centra a akcelerované výpočty se staly základní infrastrukturou evropské ekonomiky. Dostupnost výpočetní kapacity ovlivňuje schopnost podniků zavádět AI, možnosti evropského výzkumu, kvalitu digitálních veřejných služeb i bezpečnost kritických systémů.

Komise návrhem reaguje na omezenou a geograficky koncentrovanou kapacitu datových center, slabší pozici evropských cloudových poskytovatelů a právní a provozní rizika spojená se závislostí na omezeném počtu dodavatelů. CADA proto kombinuje podporu výzkumu a inovací, rozvoj infrastruktury, veřejné zadávání a nový rámec cloudové suverenity.[4]

Digital Council souhlasí se základní diagnózou Komise. Evropa potřebuje větší domácí kapacitu, více konkurenceschopných poskytovatelů a vyšší schopnost chránit citlivé systémy. Samotný tržní podíl, země původu dodavatele nebo formální umístění infrastruktury však nejsou spolehlivým měřítkem bezpečnosti.

Technologická suverenita má být posuzována podle skutečné schopnosti zákazníka:

- kontrolovat data, přístupová oprávnění a šifrovací klíče;
- zajistit kontinuitu a obnovu provozu;
- přenést data a služby k jinému poskytovateli;
- využívat otevřené standardy a interoperabilní architekturu;
- nezávisle ověřit právní, technické a organizační záruky;
- vyhnout se nepřiměřené závislosti na jediném dodavateli.

Takto pojatá suverenita je slučitelná s otevřeným trhem. Evropa může rozvíjet vlastní technologie a zároveň bezpečně spolupracovat s důvěryhodnými partnery. Přehnaně extenzivní pojetí suverenity by naopak mohlo Evropu připravit o přístup ke špičkovým technologiím, které jsou důležité i pro rozvoj samostatných evropských řešení.

2. Datová centra: správná ambice, náročná implementace

CADA předpokládá vznik akceleračních zón pro datová centra, jednotná informační místa a maximálně dvanáctiměsíční povolovací proces po předložení úplné žádosti.

Členské státy mají při výběru zón zohlednit energetickou kapacitu, konektivitu, využití odpadního tepla, environmentální dopady a možnost využít brownfieldy.[5]

Digital Council tuto část návrhu podporuje. Předvídatelnější povolování může snížit investiční nejistotu a pomoci rozšířit evropskou výpočetní kapacitu. Administrativní zrychlení však samo nevyřeší nedostatek elektřiny a síťového připojení.

Akcelerační zóny proto mají být navázány na:

- věrohodný plán rozvoje energetické sítě;
- transparentní informace o dostupné a rezervované kapacitě;
- opatření proti spekulativním rezervacím připojení;
- flexibilní spotřebu, ukládání energie a vlastní výrobu;
- využití odpadního tepla a preferenci brownfieldů;
- vysokorychlostní konektivitu;
- měřitelný přínos pro evropský technologický a výzkumný ekosystém.

Nová datová centra nemají být hodnocena pouze podle instalovaného příkonu nebo objemu investice. Podpora strategických projektů má zohledňovat také dostupnost výpočetní kapacity pro evropské podniky, startupy, výzkumné organizace a veřejnou správu. Jinak hrozí, že Evropa sice formálně navýší kapacitu infrastruktury, ale nevytvoří dostatečný přístup k výpočetním zdrojům pro subjekty, které mají tvořit evropskou inovační základnu.

3. Rámec suverenity musí být proporcionální

Návrh nařízení sleduje legitimní cíl posílení digitální suverenity Evropské unie a zvýšení odolnosti veřejného sektoru vůči bezpečnostním rizikům. Současně však existuje významné riziko, že příliš široce nastavený rámec povede k vytvoření odděleného technologického trhu pro veřejný sektor, což by mělo negativní dopady na hospodářskou soutěž, inovace a fungování jednotného vnitřního trhu.

Řada poskytovatelů softwaru a digitálních služeb dnes staví své produkty na standardizovaných cloudových platformách a cloudových službách, které nejsou využívány pouze jako infrastruktura, ale také jako zdroj databázových, analytických, bezpečnostních a AI funkcí. Pokud budou pro veřejný sektor vyžadována technologicky odlišná řešení, může to pro dodavatele znamenat nutnost přepracovat architekturu aplikací, nahradit využívané cloudové služby, vytvořit samostatné provozní procesy, bezpečnostní audity i podporu.

Toto riziko je zvlášť významné pro startupy a malé a střední podniky. Jejich konkurenční výhodou je schopnost rychle vyvíjet produkty s využitím standardizovaných cloudových služeb. Povinnost provozovat samostatnou architekturu pouze pro veřejný sektor může převýšit ekonomický přínos účasti ve veřejných zakázkách. Řada inovativních firem by se proto mohla rozhodnout veřejný sektor vůbec neobsluhovat, nebo by v něm vystupovala pouze jako subdodavatel velkých systémových integrátorů.

Výsledkem by mohlo být omezení konkurence, vyšší náklady pro stát, nižší kvalita digitálních veřejných služeb a menší zapojení inovativních firem, což by bylo v rozporu s cílem CADA podporovat evropský digitální ekosystém a účast SME ve veřejných zakázkách.

Evropská komise by proto měla výslovně posoudit dopady návrhu na startupy, malé a střední podniky a přeshraniční poskytování digitálních služeb. Požadavky na cloudovou suverenitu mají být odvozeny od skutečné citlivosti konkrétních dat, služeb a pracovních zátěží, nikoli plošně aplikovány na celé organizace nebo celé informační systémy.

3.1 Společné úrovně mohou omezit fragmentaci

CADA zavádí čtyři úrovně záruk. Úroveň 1 je založena na vlastním posouzení shody poskytovatelem, zatímco vyšší úrovně vyžadují nezávislý audit a uznání příslušným orgánem. Uznané služby mají být evidovány ve společném evropském registru.[6]

Jednotný rámec může nahradit rozdílné národní definice a otevřít poskytovatelům širší evropský trh. Tento přínos se však ztratí, pokud členské státy začnou přidávat vlastní požadavky, audity a procesy.

Výsledné nařízení má proto zajistit plné vzájemné uznávání, společné auditní důkazy a zákaz národního gold-platingu v oblastech pokrytých CADA. Smyslem evropského rámce má být méně fragmentace, nikoli její přesun z národní úrovně do paralelních certifikačních, auditních a zadávacích postupů.

3.2 Úroveň 1 nemá být plošným pravidlem pro všechna data a provozní údaje

Podmínky úrovně 1 zahrnují evropské umístění příslušné infrastruktury a výlučné uchovávání zákaznických dat, metadat a telemetrie v EU, pokud veřejný zákazník výslovně nestanoví jinak. Současně mají tuto úroveň využívat i veřejní zadavatelé pro služby, které nebyly vyhodnoceny jako relevantní pro ochranu veřejného pořádku.[7]

Digital Council doporučuje úroveň 1 přeformulovat. Základní evropský standard má vyžadovat především vysokou úroveň kybernetické bezpečnosti, transparentnost umístění a přístupů, evropskou datovou rezidenci zákaznických dat, šifrování, přenositelnost a plány kontinuity.

Evropská datová rezidence zákaznických dat je u úrovně 1 legitimním nástrojem podpory evropského cloudového a AI ekosystému. Odlišně je však třeba posuzovat metadata, telemetrii a provozní údaje. Tyto údaje mohou mít různou citlivost a technickou funkci, včetně bezpečnostního monitoringu, provozní podpory, detekce incidentů nebo zajištění dostupnosti služby.

Výlučná evropská lokalizace metadat a telemetrie má být vyžadována tehdy, pokud ji odůvodňuje povaha dat, konkrétní riziko nebo rozhodnutí veřejného zákazníka. U běžných systémů musí být možné použít také rovnocenné technické, organizační a právní záruky, zejména transparentnost, minimalizaci, účelové omezení, auditovatelnost, šifrování, zákaznickou kontrolu a omezení přístupu.

3.3 Efektivní kontrola a exteritoriální právní rizika

Debata o cloudové suverenitě se nevyhnutelně dotýká exteritoriálního dosahu zahraničních právních předpisů, zejména amerického CLOUD Actu. Digital Council považuje tato rizika za legitimní a relevantní. Neměla by však vést k mechanickému závěru, že bezpečnost lze posoudit pouze podle sídla, původu kapitálu nebo vlastnické struktury poskytovatele.

Rozhodující má být koncept efektivní kontroly. Ten zahrnuje zejména to, kdo má faktický přístup k datům, kdo spravuje šifrovací klíče, jak je řízen vzdálený přístup, jak jsou odděleny evropské provozní procesy, jaké právní závazky poskytovatel přijímá vůči zákazníkovi a jaké má zákazník možnosti auditu, kontroly, přenositelnosti a ukončení služby.

Tento přístup zároveň pomáhá zabránit tzv. „sovereignty-washingu“, tedy situaci, kdy je služba prezentována jako suverénní pouze na základě marketingového tvrzení, lokální adresy nebo formálního partnerství, aniž by zákazník měl skutečnou kontrolu nad daty, přístupy, provozem a možností změnit dodavatele.

3.4 Vyšší úrovně mají chránit skutečně kritické služby

Přísnější požadavky mohou být legitimní u obrany, zpravodajských informací, vnitřní bezpečnosti, trestního řízení nebo systémů, jejichž výpadek by přímo ohrozil základní funkce státu.

Návrh u úrovně 4 již částečně směřuje k ochraně skutečně kritických služeb. Tento princip je však třeba výslovně zachovat i při praktické klasifikaci systémů a zabránit jeho rozšiřování na celé organizace nebo komplexní systémy bez rozlišení pracovních zátěží.

Vyšší úroveň musí být vždy:

- spojena s konkrétní službou nebo pracovní zátěží;
- založena na doloženém riziku;
- omezena na nezbytný rozsah;
- pravidelně přezkoumávána;
- doprovázena hodnocením dostupnosti odpovídajících řešení na trhu.

CADA má podporovat segmentaci systémů, multi-cloud a hybridní architektury. Požadavek, aby celý komplexní systém splňoval nejvyšší úroveň, může být nákladnější a méně odolný než rozdělení jeho částí podle skutečného rizika.

U nejkritičtějších služeb spadajících do úrovně 4 může být požadavek na evropsky kontrolovaného operátora opodstatněný. Musí však být přesně omezen na skutečně kritické pracovní zátěže a nemá být automaticky přenášen do nižších úrovní ani do běžných veřejných zakázek.

3.5 Společná metodika nesmí potlačit subsidiaritu ani fragmentovat vnitřní trh

Členské státy mají pravidelně posuzovat veřejné činnosti využívající cloud a určit odpovídající úroveň záruk. Komise má připravit společnou metodiku a podle návrhu může prováděcím aktem stanovit jinou úroveň, pokud národní hodnocení považuje za nevhodné.[8]

Společná metodika je důležitá pro jednotný trh. Bez dostatečně harmonizovaných kritérií hrozí, že stejné nebo podobné veřejné služby budou v jednotlivých členských státech klasifikovány odlišně. Informační systémy pro místní samosprávu, zdravotnictví, školství, daňovou správu nebo správní agendy by tak mohly v jednom státě spadat do nižší úrovně a v jiném do výrazně přísnějšího režimu.

To by komplikovalo přeshraniční poskytování služeb, zvyšovalo compliance náklady, oslabovalo vznik evropského trhu cloudových a AI služeb a vytvářelo nejistotu pro veřejné zadavatele i dodavatele. Digital Council proto podporuje společná evropská kritéria, jednotnou metodiku a orientační typový katalog veřejných služeb a pracovních zátěží.

Současně však nesmí dojít k nahrazení národního bezpečnostního úsudku rutinním rozhodováním Komise. Pravomoc Komise změnit klasifikaci stanovenou členským státem má být omezena jasnými zákonnými kritérii, povinnou konzultací s členským státem, ochranou citlivých informací, odůvodněním a možností soudního přezkumu. U záležitostí spadajících přímo do národní bezpečnosti má Komise vydávat doporučení, nikoli automaticky závazné rozhodnutí.

3.6 Migrační lhůty musí odpovídat realitě

Návrh požaduje, aby byla migrace vyvolaná novým posouzením rizik dokončena nejpozději do 12 měsíců.[9]

Taková lhůta nemusí postačovat ani pro nové zadávací řízení, natož pro bezpečný převod komplexního informačního systému. U velkých veřejných systémů může být nutné změnit architekturu aplikací, přenést data, zajistit integrace, otestovat bezpečnost, validovat výkonnost, zajistit souběžný provoz a proškolit uživatele.

Digital Council doporučuje nejméně 24měsíční základní období a u kritických nebo technicky složitých systémů možnost harmonogramu v délce nejméně 36 měsíců nebo delšího individuálního plánu. Lhůta má začít běžet až v okamžiku, kdy je dostupná vhodná uznaná alternativa. Příslušný orgán musí mít možnost schválit delší harmonogram, pokud by urychlená migrace ohrozila kontinuitu, bezpečnost nebo integritu veřejné služby.

3.7 Soukromý sektor vyžaduje jasnější vymezení

Článek 31 umožňuje Komisi prostřednictvím aktu v přenesené pravomoci uložit posuzování a opatření také soukromým subjektům ve vysoce kritických odvětvích.[10]

Digital Council rozumí tomu, že některé soukromé subjekty, například v energetice, dopravě, zdravotnictví, bankovnictví nebo digitální infrastruktuře, plní funkce zásadní pro bezpečnost a kontinuitu společnosti. Je proto legitimní posuzovat, zda a jak se na ně mají některé požadavky CADA vztahovat.

Takové rozšíření však nesmí být neurčité. Pokud mají být povinnosti vůči soukromým subjektům ve vysoce kritických odvětvích součástí CADA, musí být jejich rozsah, kritéria, procesní záruky a vztah k NIS2, DORA a sektorovým pravidlům jasně vymezeny přímo v základním legislativním textu a podloženy posouzením dopadů. Cílem nemá být nový duplicitní compliance režim, ale jasné doplnění existujících pravidel tam, kde je to skutečně nezbytné.

Zejména ve finančním sektoru již DORA zavádí harmonizovaný rámec pro digitální provozní odolnost, řízení ICT rizik a dohled nad kritickými ICT poskytovateli třetích stran.[11] CADA proto nemá vytvářet duplicitní nebo rozporný režim, ale má navazovat na existující sektorové rámce.

4. Veřejné zakázky a evropský ekosystém

CADA zavádí kritérium evropské přidané hodnoty pro inovativní cloudové a AI zakázky. Kritérium má být spojeno s předmětem zakázky, předem zveřejněno a zůstat doplňkové, nikoli rozhodující.[12]

Digital Council tento princip podporuje. Evropská přidaná hodnota má oceňovat zejména:

- výzkum, vývoj a duševní vlastnictví vytvářené v EU;
- kvalifikovaná pracovní místa;
- bezpečnost a diverzifikaci dodavatelských řetězců;
- interoperabilitu a otevřené standardy;
- zapojení evropských startupů a SME;
- integraci technologií vzniklých z evropského výzkumu.

Kritéria nemají být založena pouze na sídle nebo vlastnické struktuře. Takový přístup by mohl znevýhodnit evropské scale-upy s mezinárodními investory a společnosti úspěšně působící na globálních trzích.

Zvláštní pozornost je třeba věnovat kritériím „zahraniční kontroly“. Pokud by byla vykládána příliš široce — například podle mezinárodního vedení firmy, přístupu k neevropskému financování, přítomnosti na neevropských trzích, příjmů od zahraničních zákazníků, akcionářské struktury, kótování na mezinárodních burzách, registrace části duševního vlastnictví mimo EU, přeshraničních datových toků nebo zaměstnávání neevropské pracovní síly — mohl by se výsledný efekt obrátit proti evropským technologickým firmám s globálními ambicemi.

Evropa potřebuje firmy, které budou schopné růst, získávat kapitál, vstupovat na světové trhy a konkurovat mimo EU. Kritéria zahraniční kontroly proto musí být jasná, úzká, přezkoumatelná a zaměřená na reálnou schopnost cizího státu nebo subjektu vynutit si přístup, ovlivnit provoz nebo narušit kontinuitu služby. Nemají trestat evropské firmy za to, že jsou úspěšné, exportně orientované nebo financované z mezinárodních zdrojů.

Návrh rovněž stanoví cíl, aby alespoň 25 % relevantních veřejných zakázek na cloudové a AI služby získaly inovativní SME.[13] Tento cíl má být podpořen především změnou zadávací praxe: dělením zakázek, modulárními architekturami, otevřenými API, přiměřenými požadavky na obrat, podporou nákladů na první audit a omezením nadměrně komplexních rámcových smluv.

EuroCloud Federation a společné nákupy mohou veřejnému sektoru pomoci sdílet kapacity a agregovat poptávku. Musí však obsahovat soutěžní pojistky, transparentní účetnictví a otevřený přístup více dodavatelů. Nadměrně velké rámcové smlouvy by mohly zvýšit koncentraci trhu a uzavřít jej menším poskytovatelům.[14]

Digital Council podporuje také využívání otevřených standardů a open-source softwaru. Open source však musí být doprovázen financováním bezpečnostních auditů, údržby a profesionální podpory. Vhodným principem je **open source first**, nikoli **open source only**.

5. Vztah CADA k existujícím rámcům

CADA nevzniká ve vakuu. Bude se uplatňovat vedle evropského rámce kybernetické certifikace, národních cloudových pravidel, NIS2, DORA, pravidel veřejného zadávání, ochrany osobních údajů a připravované či souběžné regulace digitální infrastruktury.

Regulation (EU) 2019/881, tedy Cybersecurity Act, vytvořil evropský rámec kybernetické certifikace ICT produktů, služeb a procesů.[15] CADA by měla být s tímto rámcem plně sladěna. Pokud bude poskytovatel jednou auditován nebo certifikován podle evropského certifikačního režimu, CADA nemá vytvářet duplicitní dokazování stejných skutečností.

Stejná logika platí pro DORA. Finanční sektor již podléhá harmonizovaným pravidlům pro digitální provozní odolnost, včetně řízení ICT rizik a dohledu nad kritickými ICT poskytovateli třetích stran.[16] CADA musí zabránit překryvům a rozporným požadavkům, které by zvyšovaly compliance náklady bez odpovídajícího bezpečnostního přínosu.

CADA je třeba posuzovat také společně s debatou o digitální infrastruktuře, zejména o Digital Networks Act. Rozvoj AI, cloudových služeb a datových center nebude možný bez dostupné energie, konektivity, povolovacích kapacit a odolných sítí.[17] Pravidla pro cloudovou a AI infrastrukturu proto nemají vznikat odděleně od širší politiky digitálních sítí.

V českém kontextu je zvlášť důležité sladění s katalogem cloud computingu a stávajícím systémem bezpečnostních úrovní. V katalogu jsou zveřejňovány nabídky cloud computingu, které splnily požadavky zákona č. 365/2000 Sb. pro zápis do katalogu cloud computingu, a zapsané nabídky mohou orgány veřejné správy využívat podle pravidel ZoISVS.[18] NÚKIB zároveň popisuje českou regulaci cloud computingu jako propojený systém zákona o informačních systémech veřejné správy, zákona o kybernetické bezpečnosti a navazujících cloudových vyhlášek.[19]

Výsledný CADA by proto měl obsahovat jasné přechodné mechanismy a uznávací pravidla vůči národním systémům. Poskytovatelé ani veřejní zadavatelé nemají podstupovat dvě paralelní posouzení stejných rizik.

6. Priority pro Českou republiku

CADA může České republice přinést nové investice, přístup k evropské výpočetní kapacitě a příležitosti pro české poskytovatele cloudu, kybernetické bezpečnosti a softwaru. Současně však vytvoří významné implementační nároky na veřejnou správu.

Česká republika již používá vlastní systém bezpečnostních úrovní a katalog cloudových služeb. Klíčovou prioritou proto musí být sladění českého a evropského rámce. Poskytovatelé ani veřejní zadavatelé nemají podstupovat dvě paralelní posouzení stejných rizik.

Stejně důležité je sladění CADA s existujícími evropskými a sektorovými pravidly, zejména NIS2, DORA, evropskými certifikačními režimy a připravovanými pravidly pro digitální infrastrukturu. Česká pozice má prosazovat princip „one audit – many uses“ a zabránit duplicitnímu compliance tam, kde již existují srovnatelné technické, bezpečnostní nebo sektorové požadavky.

Česká vláda by měla během legislativního projednávání:

1. porovnat evropské úrovně s českými bezpečnostními pravidly;
2. zmapovat veřejné systémy a existující cloudové smlouvy;
3. předběžně určit, které systémy mohou vyžadovat vyšší úroveň;

4. odhadnout náklady, kapacity a čas potřebný pro případné migrace;
5. připravit společnou pozici odpovědných ministerstev, DIA a NÚKIB;
6. analyzovat vhodné lokality pro datová centra podle dostupnosti energie, konektivity, brownfieldů a využití odpadního tepla;
7. konzultovat návrh s poskytovateli, veřejnými zadavateli, SME, energetikou a výzkumnými organizacemi;
8. připravit zásady pro veřejné zakázky podporující modularitu, otevřená API a účast SME;
9. vytvořit přechodový plán pro sladění katalogu cloud computingu s budoucím evropským registrem;
10. prosazovat princip „one audit – many uses“ na evropské i národní úrovni.

Česká pozice by měla spojovat podporu evropských kapacit s důrazem na proporcionalitu, právní jistotu a proveditelnost. Cílem nemá být pouze změna struktury veřejných zakázek, ale bezpečnější a rychlejší modernizace státu a lepší podmínky pro růst českých technologických firem.

Česká republika by měla zvlášť prosazovat, aby technologická suverenita nebyla interpretována jako izolace od transatlantických partnerů. Pro otevřenou ekonomiku je důležité posilovat evropské kapacity, ale zároveň zachovat přístup k nejlepším technologiím, kapitálu, know-how a bezpečnostní spolupráci s důvěryhodnými partnery.

Digital Council

Závěr

Cloud and AI Development Act přichází ve chvíli, kdy Evropa potřebuje zvýšit investice do výpočetní infrastruktury, urychlit adopci AI a snížit kritické jednostranné závislosti. Jeho strategický směr si proto zaslouží podporu.

Výsledné nařízení však nesmí zaměnit suverenitu za izolaci, lokalizaci za bezpečnost nebo omezení soutěže za inovaci. Přísné požadavky mají být soustředěny na služby, u nichž jsou skutečně nezbytné. Běžná veřejná správa musí mít přístup k bezpečným, moderním a konkurenceschopným technologiím.

Evropská datová rezidence zákaznických dat u úrovně 1 může být rozumným nástrojem podpory evropského cloudového a AI ekosystému. Nemá se však automaticky rozšiřovat na všechna metadata, telemetrii a provozní údaje bez rozlišení jejich citlivosti a funkce. U nejkritičtější úrovně 4 může být evropská kontrola operátora legitimní, ale pouze jako úzce vymezený bezpečnostní nástroj pro skutečně kritické pracovní zátěže.

CADA musí zároveň vytvořit reálné příležitosti pro evropské startupy a SME. To vyžaduje modulární zadávání, otevřené standardy, dostupné audity a pravidla, která odměňují skutečnou evropskou technologickou a ekonomickou činnost. Příliš široká kritéria zahraniční kontroly by naopak mohla poškodit právě ty evropské firmy, které mají ambici růst globálně.

Úspěch CADA se nebude měřit počtem nových povinností ani počtem služeb označených za suverénní. Rozhodující bude, zda Evropa získá více bezpečné a udržitelné výpočetní kapacity, větší nabídku konkurenceschopných technologií, nižší závislost na jednotlivých dodavatelích a odolnější veřejné služby.

Evropa nepotřebuje digitální izolaci. Potřebuje vlastní kapacity, schopnost volby, kontrolu nad kritickými závislostmi a otevřený ekosystém důvěryhodných partnerů. Na těchto principech by měl být výsledný CADA postaven.

Digital Council

Poznámky pod čarou

[1] Evropská komise, *Proposal for a Regulation establishing a framework of measures for strengthening Europe's cloud and AI ecosystem*, COM(2026) 502 final, 3. 6. 2026; Evropský parlament, procedura 2026/0138(COD), stav k 13. 7. 2026.

[2] Evropská komise, COM(2026) 502 final, čl. 30 a příloha II, Union assurance level 1.

[3] Evropská komise, COM(2026) 502 final, čl. 29 odst. 6.

[4] Evropská komise, COM(2026) 502 final, důvodová zpráva, s. 1–4.

[5] Evropská komise, COM(2026) 502 final, čl. 10–14.

[6] Evropská komise, COM(2026) 502 final, čl. 16–22.

[7] Evropská komise, COM(2026) 502 final, čl. 30 odst. 2 a příloha II.

[8] Evropská komise, COM(2026) 502 final, čl. 29 odst. 3–5.

[9] Evropská komise, COM(2026) 502 final, čl. 29 odst. 6.

[10] Evropská komise, COM(2026) 502 final, čl. 31 odst. 3.

[11] Nařízení Evropského parlamentu a Rady (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru.

[12] Evropská komise, COM(2026) 502 final, čl. 32.

[13] Evropská komise, COM(2026) 502 final, čl. 33 odst. 4.

[14] Evropská komise, COM(2026) 502 final, čl. 34–40.

[15] Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019, Cybersecurity Act.

[16] Nařízení Evropského parlamentu a Rady (EU) 2022/2554, DORA.

[17] Evropská komise, *The Digital Networks Act*, 21. 1. 2026.

[18] Digitální a informační agentura, *Nabídky cloud computingu*, katalog cloud computingu podle ZoISVS.

[19] NÚKIB, *Strategická analýza: Cloud Computing*, 15. 3. 2024.