Digital Council

Pozice Digital Council k ochraně datové suverenity EU

Digital Council

Úvod

Digital Council podporuje cíl Evropské komise posílit datovou suverenitu Evropské unie. Datovou suverenitu však nelze redukovat na fyzické umístění dat v EU ani na původ poskytovatele technologie. Správně chápaná datová suverenita znamená schopnost evropských firem, veřejných institucí a občanů mít účinnou kontrolu nad tím, kdo k datům přistupuje, za jakých podmínek, v jaké jurisdikci, s jakými technickými zárukami a s jakou možností změnit poskytovatele nebo provozní model.

Evropa potřebuje bezpečné a důvěryhodné mezinárodní toky dat. Bez nich nelze rozvíjet umělou inteligenci, cloudové služby, kyberbezpečnost, výzkum, digitální veřejné služby, průmyslové datové prostory ani přeshraniční dodavatelské řetězce. Důvěryhodné přeshraniční datové toky jsou zásadní také pro prevenci podvodů, boj proti finanční kriminalitě, globální sdílení threat intelligence, monitoring rizik v reálném čase a kontinuitu podnikání.

Současně geopolitické prostředí, asymetrie v přístupu na trhy, požadavky třetích zemí na lokalizaci nebo zpřístupnění dat a rizika neoprávněného přístupu k citlivým neosobním datům vyžadují od EU aktivnější a strategičtější přístup.

Digital Council doporučuje, aby EU postupovala na základě rizik, technologicky neutrálně a proporcionálně. Opatření mají chránit skutečně citlivé kategorie dat a kritické use-cases, nikoli vytvářet plošné překážky pro běžné obchodní, výzkumné, provozní a bezpečnostní datové toky.

Jádrem evropské datové suverenity by měly být právní jistota, interoperabilita, otevřené standardy, auditovatelnost, zákaznická kontrola šifrovacích klíčů, transparentnost privilegovaných přístupů, cloud switching, přenositelnost, reverzibilita, odolnost dodavatelských řetězců a vymahatelné smluvní záruky.

Evropská politika datové suverenity má konkurenceschopnost posilovat, nikoli oslabovat. Nová pravidla proto nesmí přidat další složitou compliance vrstvu nad GDPR, Data Act, Data Governance Act, NIS2, Cyber Resilience Act, DORA a sektorové předpisy. Musí být srozumitelná, prakticky proveditelná a použitelná i pro startupy, malé a střední podniky a menší veřejné zadavatele.

Digital Council

Základní východisko: suverenita jako kontrola, nikoli izolace

Digital Council doporučuje, aby EU definovala datovou suverenitu jako schopnost účinné kontroly, nikoli jako izolaci nebo plošnou lokalizaci.

Fyzické umístění dat v EU může být relevantní u některých citlivých use-cases. Samo o sobě však nezajišťuje suverenitu. Data mohou být uložena v EU, a přesto může existovat riziko neoprávněného přístupu prostřednictvím vzdálené správy, subdodavatelského řetězce, privilegovaných administrátorských účtů, právních povinností poskytovatele v třetí zemi nebo nedostatečné kontroly nad šifrovacími klíči.

Naopak některé přeshraniční datové toky mohou být bezpečné, legitimní a nezbytné, pokud jsou podloženy jasným právním titulem, smluvními zárukami, technickými opatřeními, transparentností a auditovatelností. Cílem EU by proto nemělo být udržet všechna data v Evropě za každou cenu, ale zajistit, aby evropské organizace mohly vědomě rozhodovat, kde a jak jsou jejich data zpracovávána, kdo k nim má přístup a jaké mají možnosti kontroly, nápravy a odchodu.

Digital Council navrhuje pracovat s pěti dimenzemi datové suverenity:

Právní kontrola znamená jasné určení toho, jaké právo se použije, kdo může data vyžadovat nebo zpřístupnit, jak se řeší požadavky orgánů třetích zemí a zda existují účinné opravné prostředky.

Technická kontrola zahrnuje šifrování, správu klíčů, identity management, logování, monitoring, řízení privilegovaných přístupů, segmentaci prostředí a bezpečnostní architekturu.

Provozní kontrola znamená schopnost zajistit kontinuitu služeb, obnovu po incidentu, odolnost proti výpadkům, krizové řízení a fungující exit plán.

Ekonomická kontrola spočívá v možnosti změnit poskytovatele, přenést data a workloady, vyhnout se nepřiměřenému vendor lock-inu a využívat interoperabilní řešení.

Institucionální kontrola znamená auditovatelnost, dohled, certifikaci, vymahatelnost pravidel a jasné kompetence mezi orgány EU, členskými státy, regulátory a zadavateli.

Digital Council

Ochrana citlivých neosobních dat

Digital Council podporuje záměr Komise lépe chránit citlivá neosobní data. Některá neosobní data mohou mít významnou hospodářskou, bezpečnostní nebo strategickou hodnotu. Jde například o data z kritické infrastruktury, průmyslová výrobní data, kyberbezpečnostní telemetrii, technická data ze strategických sektorů, vybraná výzkumná data, data veřejné správy nebo datasety využitelné pro trénování a validaci AI systémů.

Data Act již obsahuje pravidla, podle nichž poskytovatelé služeb zpracování dat musí přijmout přiměřená technická, organizační a právní opatření proti mezinárodnímu a třetizemskému vládnímu přístupu k neosobním datům drženým v EU, pokud by takový přístup nebo předání bylo v rozporu s právem EU nebo právem členského státu.[4]

Digital Council však varuje před vytvořením příliš široké nebo neurčité kategorie „strategických dat“. Pokud by nebyla přesně vymezena, mohla by zasáhnout běžné podnikové procesy, zvýšit compliance náklady a vytvořit právní nejistotu pro firmy i veřejné instituce.

EU by měla zavést praktickou klasifikaci rizik založenou na těchto kritériích:

1. povaha dat a jejich citlivost;
2. sektor a význam pro veřejný zájem;
3. pravděpodobnost a dopad zneužití;
4. dostupnost technických a smluvních záruk;
5. expozice vůči právu třetích zemí;
6. dopad na konkurenceschopnost, inovace a provozní kontinuitu;
7. možnost anonymizace, pseudonymizace, agregace, federovaného zpracování nebo využití syntetických dat;
8. dostupnost privacy-enhancing technologies a dalších technických kontrol, které mohou snížit potřebu přesunu nebo zpřístupnění dat.

Zvýšená ochrana by měla být vyhrazena pro konkrétní rizikové use-cases, nikoli aplikována plošně na celé sektory nebo všechny přeshraniční datové toky. EU by zároveň měla poskytnout regulatorní jistotu, že privacy-enhancing technologies, silné šifrování, zákaznická kontrola klíčů, secure multi-party computation, data clean rooms, federované učení a další záruky mohou být tam, kde je to vhodné, uznány jako smysluplná opatření ke snížení rizika.

Digital Council

Mezinárodní datové toky: otevřenost s důvěrou

Digital Council podporuje princip „data free flow with trust“. Přeshraniční datové toky jsou základní podmínkou fungování digitální ekonomiky. Jsou nezbytné pro cloud, AI, kyberbezpečnost, výzkum, finanční služby, e-commerce, průmyslové dodavatelské řetězce, zákaznickou podporu, vzdálenou správu i spolupráci mezi firmami a veřejnými institucemi.

Jsou rovněž nepostradatelné pro prevenci podvodů, boj proti finanční kriminalitě a kybernetickou odolnost. Moderní monitoring podvodů a kybernetických rizik často závisí na schopnosti identifikovat globální vzorce, sdílet threat intelligence, detekovat anomálie v reálném čase a udržovat geograficky distribuovanou infrastrukturu. Příliš restriktivní lokalizační požadavky proto mohou odolnost a provozní efektivitu snižovat, nikoli zvyšovat.

U osobních údajů již existuje široká sada nástrojů podle kapitoly V GDPR, včetně rozhodnutí o odpovídající ochraně, standardních smluvních doložek, závazných podnikových pravidel, certifikačních mechanismů, kodexů chování a výjimek.[5] U neosobních dat by EU měla vytvořit obdobně srozumitelný, ale přiměřený rámec pro identifikaci a řízení rizik, aniž by vznikala zbytečná duplicita s existujícími pravidly.

EU by měla aktivně reagovat tam, kde třetí země ukládají evropským subjektům neodůvodněné lokalizační požadavky, omezují export dat, diskriminují evropské poskytovatele, podmiňují přístup na trh sdílením citlivých dat nebo neposkytují dostatečné záruky proti neoprávněnému vládnímu přístupu. Reakce EU by však měla být odstupňovaná: přednost mají mít diplomacie, regulatorní dialog, obchodní dohody, standardy, vzájemné uznávání a interoperabilní mosty. Restriktivní opatření by měla být využívána až tam, kde strukturální nerovnováhy nebo zneužívání otevřenosti EU přetrvávají.

Komise by měla nadále podporovat důvěryhodné a škálovatelné mechanismy pro mezinárodní předávání dat, včetně rozhodnutí o odpovídající ochraně tam, kde jsou vhodná, standardních smluvních doložek, závazných podnikových pravidel, certifikačních mechanismů, kodexů chování a dalších důvěryhodných transferových nástrojů. Adekvátnost zůstává hodnotným nástrojem, ale nemůže být jediným pilířem evropské mezinárodní datové strategie. Moderní ekonomika založená na AI a cloudu potřebuje širší, odolnější a operativněji využitelnou architekturu pro předávání dat.

Digital Council

Praktické překážky na trzích třetích zemí

Evropské firmy působící globálně stále častěji čelí dvojímu tlaku. Na jedné straně se na zahraničních trzích setkávají s požadavky na lokalizaci dat, očekáváním lokálního zpracování, regulatorními schváleními, sektorovým licencováním, bezpečnostními prověrkami nebo podmínkami veřejných zakázek, které mohou fungovat jako překážky vstupu na trh. Na druhé straně musí současně plnit složité evropské požadavky na předávání dat, včetně individuálních posouzení, která mohou být v praxi obtížně aplikovatelná, zejména pro menší subjekty.

Praktické výzvy ilustruje několik významných trhů. Čínský rámec pro přeshraniční předávání dat zahrnuje u některých odchozích přenosů cestu bezpečnostního posouzení, standardní smlouvy nebo certifikace. Indie vyžaduje, aby poskytovatelé platebních systémů uchovávali data platebních systémů v Indii. Turecko zavedlo vlastní standardní smlouvy pro předávání dat do zahraničí. Uruguay umožňuje modelové smluvní doložky pro mezinárodní přenosy, ale v určitých případech může být stále vyžadováno předchozí povolení. Saúdská Arábie a Spojené arabské emiráty přijaly režimy předávání dat, které pro přenosy do zahraničí stanoví specifické podmínky nebo záruky. Jihoafrické rámce pro veřejné zakázky a datovou/cloudovou politiku rovněž ukazují, jak mohou cíle v oblasti lokálního obsahu, místní inkorporace nebo domácích kapacit interagovat s přístupem na trh a procurementem.[6]

Tato opatření se liší účelem, právním nastavením i intenzitou. Nelze je považovat za totožná. Dohromady však ukazují širší trend: pravidla pro předávání dat, lokalizační očekávání, licenční požadavky, procurementové preference a požadavky na lokální právní entitu mohou kumulativně zvyšovat náklady, zpomalovat vstup na trh, snižovat rychlost uzavírání obchodů, fragmentovat globální architekturu řízení rizik a vytvářet tlak na duplikaci infrastruktury.

To je problematické zejména v sektorech, jako jsou platby, kyberbezpečnost, cloudové služby a AI, kde odolnost závisí na integrovaném monitoringu, globální expertize, real-time analytice a schopnosti fungovat napříč jurisdikcemi. EU by proto měla překážky ve třetích zemích řešit prostřednictvím obchodní politiky, digitálních partnerství, regulatorních dialogů a mezinárodní standardizace, ale zároveň se vyvarovat opatření, která by tytéž překážky replikovala uvnitř jednotného trhu.

Digital Council

Zjednodušení evropské governance předávání dat

EU by se měla podívat také dovnitř. Důvěryhodná politika datové suverenity nemůže pouze reagovat na překážky ve třetích zemích; musí zároveň zajistit, aby pravidla EU byla koherentní, předvídatelná a prakticky použitelná.

Současný rámec pro mezinárodní předávání osobních údajů je často vnímán jako právně složitý a provozně zatěžující. Transfer Impact Assessments, rozdílné výklady dozorových orgánů, zdlouhavé schvalování závazných podnikových pravidel a překrývající se smluvní požadavky mohou vytvářet nepřiměřené náklady, zejména pro SME, školy, veřejné instituce a menší poskytovatele služeb. V některých případech jsou organizace fakticky nuceny posuzovat zahraniční surveillance laws s mírou právní sofistikovanosti, která je mimo velké nadnárodní compliance týmy nerealistická.

Digital Council proto podporuje přístup orientovaný na zjednodušení. Komise by měla posoudit, zda lze existující mechanismy kapitoly V GDPR učinit škálovatelnějšími a předvídatelnějšími, včetně těchto kroků:

- umožnit portfoliová nebo skupinová posouzení pro podobné přenosy využívající stejné záruky;
- vyjasnit, že pro posuzování přenosů je relevantní praktická pravděpodobnost a skutečné riziko přístupu zahraničních orgánů, nikoli neproveditelný zero-risk standard;
- zjednodušit a urychlit schvalování BCR, včetně jasnějších lhůt a silnějšího vzájemného uznávání mezi dozorovými orgány;
- aktualizovat a rozšířit standardní smluvní nástroje tam, kde vznikají právní mezery nebo duplicitní uspořádání;
- urychlit kodexy chování a certifikační mechanismy podle článků 40 a 42 GDPR pro cloudové služby a mezinárodní přenosy;
- poskytnout jasné vodítko k roli privacy-enhancing technologies jako uznávaných záruk;
- omezit duplicitní smluvní požadavky tam, kde již existují ekvivalentní záruky.

Tento přístup by měl být rámován jako zjednodušení a operacionalizace existujících právních nástrojů, nikoli jako snižování ochrany. Cílem má být zachovat vysokou úroveň ochrany a současně učinit důvěryhodné datové toky prakticky zvládnutelnými.

www.digitalcouncil.eu
prague@digitalcouncil.eu

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

Digital Council

Lokalizace dat: legitimní nástroj pouze v omezených případech

Plošná datová lokalizace by neměla být výchozím nástrojem evropské politiky datové suverenity. Lokalizace může být legitimní u úzké skupiny kritických use-cases, například u některých obranných, bezpečnostních, justičních, zdravotních, energetických nebo vysoce citlivých veřejnosprávních systémů. I v těchto případech však musí být odůvodněná konkrétním rizikem, technologicky proveditelná, právně přezkoumatelná a doprovázená požadavky na kyberbezpečnost, interoperabilitu a reverzibilitu.

U běžných komerčních, výzkumných, provozních a bezpečnostních datových toků by plošná lokalizace pravděpodobně vedla k vyšším nákladům, fragmentaci trhu, nižší dostupnosti služeb a omezení inovací. Mohla by také nepřiměřeně zasáhnout startupy a malé a střední podniky, které často využívají globální cloudovou infrastrukturu právě proto, že jim umožňuje škálovat rychleji a levněji.

EU by proto měla rozlišovat mezi:

- **data residency**, tedy umístěním dat v určité jurisdikci;
- **operational sovereignty**, tedy kontrolou nad provozem, privilegovanými přístupy a kontinuitou služeb;
- **legal sovereignty**, tedy schopností bránit neoprávněnému přístupu nebo konfliktu právních režimů;
- **technical sovereignty**, tedy zákaznickou kontrolou klíčů, architektury, logování a bezpečnostních opatření;
- **economic sovereignty**, tedy možností přenést data a změnit poskytovatele.

Toto rozlišení je klíčové. Bez něj hrozí, že EU přijme formálně „suverénní" pravidla, která ve skutečnosti neposílí kontrolu nad daty, ale pouze zvýší náklady a administrativní zátěž.

Cloud, AI a vendor lock-in

Jedním z největších praktických rizik pro evropské firmy a veřejné instituce není pouze místo uložení dat, ale to, zda lze data, aplikace a workloady efektivně přesunout. Skutečná datová suverenita vyžaduje možnost změnit poskytovatele, kombinovat více poskytovatelů, využívat hybridní architektury a vyhnout se situaci, kdy technická závislost na jednom ekosystému znemožní racionální rozhodování.

Digital Council

Data Act posiluje pravidla pro switching mezi poskytovateli služeb zpracování dat, včetně cloudových a edge služeb, a stanoví rámec pro přenositelnost dat, digitálních aktiv a interoperabilitu. Zároveň požaduje, aby poskytovatelé odstraňovali překážky switchingu, a od ledna 2027 postupně ruší switching charges, včetně poplatků za odchozí přenos dat.[7]

Digital Council doporučuje, aby Komise v oblasti datové suverenity kladla zvláštní důraz na:

- export dat ve standardizovaných a strojově čitelných formátech;
- otevřená API a interoperabilitu;
- technickou reverzibilitu služeb;
- smluvně zakotvené exit plány;
- zákaz nepřiměřených egress fees a skrytých switching nákladů;
- zákaznickou kontrolu šifrovacích klíčů;
- transparentní seznam subdodavatelů;
- auditovatelná logování přístupů;
- jasnou odpovědnost mezi poskytovatelem, zákazníkem a subdodavateli;
- podporu otevřených standardů a open source komponent tam, kde jsou bezpečné, udržitelné a ekonomicky realistické.

Cloudová a AI infrastruktura bude pro evropskou ekonomiku stejně strategická jako energetická, dopravní nebo finanční infrastruktura. Evropská politika proto musí podporovat rozvoj vlastních kapacit, ale neměla by bránit přístupu k nejlepším dostupným technologiím od důvěryhodných poskytovatelů. Cílem má být větší schopnost volby, nikoli administrativně vytvořená závislost na užším okruhu dodavatelů.

Původ poskytovatele nemá nahrazovat měřitelné bezpečnostní záruky

U citlivých use-cases může být relevantní hodnotit jurisdikční riziko, vlastnickou strukturu, kontrolu nad provozem, dodavatelské řetězce nebo expozici vůči právu třetích zemí. Digital Council však nedoporučuje používat původ firmy jako jednoduchou náhradu za měřitelné bezpečnostní, právní a provozní záruky.

Evropský původ poskytovatele automaticky nezaručuje vysokou úroveň bezpečnosti, interoperability nebo provozní odolnosti. Mimoevropský původ poskytovatele automaticky neznamená nepřijatelné riziko. Rozhodující má být konkrétní risk assessment: kdo ovládá infrastrukturu, kdo spravuje klíče, kdo má privilegované

přístupy, jak jsou řešeny požadavky orgánů třetích zemí, jaké existují smluvní a technické bariéry proti neoprávněnému přístupu a jaké jsou možnosti auditu a nápravy.

Návrh Cloud and AI Development Act předpokládá celoevropský rámec pro posuzování cloudové a AI suverenity, včetně úrovní suverénních záruk, které obsahují kritéria týkající se zpracování v Unii, nezávislosti na třetích zemích a na vyšších úrovních také vlastnictví a kontroly v EU, spolu s možností uznání poskytovatelů ze třetích zemí.[8] O to důležitější je, aby byla kritéria suverenity aplikována pečlivě, transparentně a proporcionálně.

Digital Council doporučuje vyvážený rámec.

U běžných služeb mají být rozhodující měřitelné bezpečnostní výsledky, interoperabilita, smluvní záruky a možnost odchodu.

U vysoce citlivých veřejných nebo kritických služeb mohou být přísnější požadavky legitimní, včetně požadavků na provozní kontrolu v EU, omezení privilegovaných přístupů ze třetích zemí, nezávislé audity nebo dedikovaná suverénní prostředí.

Takové požadavky však musí být transparentní, přiměřené, technologicky proveditelné, časově realistické a přezkoumatelné. Tam, kde budou budoucí rámce EU pro suverénní záruky interagovat s mezinárodními přenosy dat, by neměly spoléhat pouze na rozhodnutí o odpovídající ochraně, ale měly by tam, kde je to vhodné, uznávat celou škálu zákonných mechanismů kapitoly V GDPR, včetně SCCs, BCRs, kodexů chování a certifikačních mechanismů.

Dopady na startupy, SME a evropskou konkurenceschopnost

Digital Council považuje konkurenceschopnost za jeden z hlavních testů jakékoli nové iniciativy v oblasti datové suverenity. Evropa již dnes čelí složitému regulatornímu prostředí. Pokud by nová pravidla přidala další nejasné povinnosti, duplicitní reporting nebo nákladné právní posuzování, nejvíce by dopadla právě na startupy, malé a střední podniky a menší veřejné instituce.

To by bylo kontraproduktivní. Datová suverenita má posilovat evropskou schopnost inovovat, nikoli vytvářet další překážky pro adopci cloudu, AI a datové analytiky. Podle Eurostatu využívalo v roce 2025 placené cloudové služby 53 % podniků v EU, což ukazuje rostoucí význam cloudu pro evropskou ekonomiku.[9] Data Union Strategy zároveň označuje zjednodušení datových pravidel za jednu ze svých hlavních priorit.[3]

Digital Council proto doporučuje zavést princip: **žádná nová povinnost bez zjednodušení**.

Nová opatření by měla být doprovázena praktickými nástroji:

- jednoduchý risk-assessment template;
- vzorové smluvní doložky;
- sektorové příklady dobré praxe;
- guidance pro startupy a SME;
- jasné rozlišení odpovědností mezi poskytovateli infrastruktury, zákazníky a zprostředkovateli;
- přechodná období;
- možnost využití certifikovaných nebo předem posouzených služeb;
- regulatorní sandboxy pro datové prostory, AI a citlivé datové use-cases;
- jednotné kontaktní místo pro výklad pravidel.

EU by měla také průběžně vyhodnocovat dopady navržených opatření na náklady, dostupnost technologií, rychlost adopce AI, investice do datové infrastruktury, startupy, SME a veřejné zadavatele.

Doporučení Digital Councilu pro Evropskou komisi

Digital Council vítá snahu Evropské komise posílit datovou suverenitu EU. Data jsou strategickým aktivem evropské ekonomiky a jejich bezpečné využívání bude zásadní pro rozvoj AI, cloudových služeb, průmyslových datových prostorů, výzkumu, veřejných služeb, prevence podvodů, kyberbezpečnosti a konkurenceschopnosti evropských firem.

Evropská politika datové suverenity by však měla být založena na kontrole, proporcionalitě a otevřenosti vůči důvěryhodným partnerům. Správným cílem není držet všechna data v Evropě bez ohledu na kontext, ale zajistit, aby evropské organizace měly reálnou kontrolu nad svými daty, transparentní záruky, vymahatelná práva a skutečnou možnost volby.

Digital Council doporučuje, aby Evropská komise:

1. Definovala datovou suverenitu jako účinnou kontrolu nad daty, nikoli jako plošnou lokalizaci

Datová suverenita by neměla být redukována na fyzické umístění dat v EU. Lokalita dat může být relevantní u některých citlivých use-cases, sama o sobě však nezajišťuje kontrolu nad přístupem, šifrovacími klíči, provozem infrastruktury, žádostmi orgánů třetích zemí ani možností změnit poskytovatele.

EU by měla pracovat s širším pojetím suverenity, které zahrnuje právní, technickou, provozní a ekonomickou kontrolu nad daty.

2. Zavedla praktickou klasifikaci citlivých neosobních dat

Digital Council podporuje cílenou ochranu citlivých neosobních dat, zejména tam, kde mají hospodářskou, bezpečnostní nebo strategickou hodnotu. Může jít například o data z kritické infrastruktury, průmyslová data, kyberbezpečnostní telemetrii, vybraná výzkumná data, data veřejné správy nebo datasety využitelné pro trénování a validaci AI systémů.

Komise by se však měla vyhnout příliš široké nebo neurčité kategorii „strategických dat“. Zvýšená ochrana má být založena na konkrétním posouzení rizika, dopadu zneužití, sektoru, technických záruk, expozice vůči právu třetích zemí a dostupných opatření ke snížení rizika, včetně privacy-enhancing technologies.

3. Zachovala důvěryhodné mezinárodní datové toky

Přeshraniční datové toky jsou nezbytné pro cloud, AI, kyberbezpečnost, prevenci podvodů, prevenci finanční kriminality, výzkum, finanční služby, e-commerce, průmyslové řetězce i zákaznickou podporu. EU by proto měla vycházet z principu „data free flow with trust“.

Evropa má být otevřená vůči důvěryhodným partnerům, ale zároveň schopná reagovat na neodůvodněné lokalizační požadavky, diskriminační pravidla, omezení exportu dat, slabé záruky proti vládnímu přístupu nebo požadavky na sdílení citlivých dat jako podmínku přístupu na trh.

4. Řešila překážky na trzích třetích zemí prostřednictvím obchodu, diplomacie a interoperability

EU by měla využívat obchodní politiku, digitální partnerství, regulatorní dialogy a mezinárodní standardizaci k řešení opatření třetích zemí, která fungují jako de facto lokalizační nebo tržní překážky. To zahrnuje situace, kdy omezení přenosů, licenční požadavky, procurementové preference, bezpečnostní prověrky nebo požadavky na lokální právní entitu nutí evropské firmy duplikovat infrastrukturu nebo fragmentovat globální provoz.

EU by měla zároveň podporovat multilaterální přístupy k důvěryhodným datovým tokům, včetně práce OECD na Data Free Flow with Trust a interoperability s globálními accountability-based rámci, jako je systém Global Cross-Border Privacy Rules.[10]

5. Používala datovou lokalizaci pouze jako výjimečný a odůvodněný nástroj

Plošná lokalizace dat by neměla být výchozím řešením evropské politiky datové suverenity. Může být legitimní u úzce vymezených kritických use-cases, například u některých obranných, bezpečnostních, energetických, zdravotních nebo vysoce citlivých veřejnosprávních systémů.

I v těchto případech musí být lokalizace podložena konkrétním rizikem, technologicky proveditelná, přezkoumatelná a doprovázená požadavky na kyberbezpečnost, interoperabilitu a reverzibilitu.

6. Posílila cloud switching, interoperabilitu a reverzibilitu

Skutečná datová suverenita vyžaduje možnost změnit poskytovatele a přenést data, aplikace a workloady bez nepřiměřených technických nebo ekonomických bariér. Suverenita bez možnosti odchodu od poskytovatele je pouze formální.

Komise by měla dále podporovat standardizované a strojově čitelné formáty, otevřená API, technickou reverzibilitu služeb, smluvně zakotvené exit plány, transparentnost subdodavatelů, auditovatelná logování přístupů a zákaznickou kontrolu šifrovacích klíčů.

7. Nepoužívala původ poskytovatele jako jednoduché bezpečnostní kritérium

U citlivých use-cases může být relevantní hodnotit jurisdikční riziko, vlastnickou strukturu, provozní kontrolu, dodavatelské řetězce nebo expozici vůči právu třetích zemí. Tato kritéria by však neměla nahrazovat konkrétní bezpečnostní, smluvní a technické záruky.

Digital Council

Evropský původ poskytovatele automaticky nezaručuje bezpečnost a mimoevropský původ automaticky neznamená nepřijatelné riziko. Rozhodující má být transparentní risk assessment, měřitelné záruky, auditovatelnost, kontrola přístupů, možnost nápravy a možnost změnit poskytovatele.

8. Operacionalizovala existující nástroje kapitoly V GDPR pro předávání dat

EU by měla nadále podporovat rozhodnutí o odpovídající ochraně, ale neměla by na nich stavět výlučně. Měla by učinit celou škálu mechanismů kapitoly V GDPR škálovatelnější a operativně využitelnou, včetně SCCs, BCRs, certifikačních mechanismů, kodexů chování a dalších důvěryhodných transferových nástrojů.

Komise by měla posoudit cílená zjednodušení, která by omezila duplicitní posuzování přenosů, zrychlila schvalování BCR, vyjasnila použití SCCs ve složitých přenosových scénářích a poskytla větší právní jistotu organizacím, které spoléhají na uznané technické záruky a privacy-enhancing technologies.

9. Zabránila duplicitě s existujícím evropským datovým rámcem

Evropský datový a digitální rámec již zahrnuje GDPR, Data Act, Data Governance Act, pravidla pro volný tok neosobních dat, NIS2, Cyber Resilience Act, DORA a sektorovou regulaci. Nová opatření k datové suverenitě by proto neměla vytvářet další paralelní compliance režim.

Digital Council doporučuje princip „žádná nová povinnost bez zjednodušení". Nová pravidla mají stávající rámec vyjasňovat a doplňovat, nikoli přidávat duplicitní reporting, nejasné odpovědnosti nebo další administrativní vrstvu.

10. Zohlednila dopady na startupy, SME a menší veřejné zadavatele

Pravidla k datové suverenitě musí být prakticky použitelná i pro organizace, které nemají rozsáhlé právní, bezpečnostní a procurement týmy. Příliš složité nebo nákladné požadavky by mohly zpomalit adopci cloudu, AI a datové analytiky právě u menších firem a institucí.

Komise by měla připravit jednoduché risk-assessment nástroje, vzorové smluvní doložky, sektorové příklady dobré praxe, guidance, přechodná období a možnost využití certifikovaných nebo předem posouzených služeb.

Digital Council

11. Podporovala evropské technologické kapacity otevřeným způsobem

Evropa potřebuje rozvíjet vlastní cloudové, AI, polovodičové, kyberbezpečnostní a open source kapacity. Tato ambice je legitimní, ale neměla by být naplňována primárně restrikcemi, které zúží konkurenci nebo omezí přístup evropských organizací k důvěryhodným technologiím.

Evropská technologická suverenita má být otevřená: jejím cílem má být větší schopnost volby, interoperabilita, kontrola nad kritickými závislostmi, odolnost dodavatelských řetězců a možnost změnit poskytovatele.

12. Pravidelně vyhodnocovala dopady na konkurenceschopnost a odolnost

Každé nové opatření v oblasti datové suverenity by mělo být posuzováno nejen z hlediska bezpečnosti, ale také podle dopadů na náklady, investice, inovace, dostupnost služeb, startupy, SME, veřejné zadavatele, prevenci podvodů, kyberbezpečnost a přeshraniční obchod.

Evropská datová suverenita bude úspěšná pouze tehdy, pokud současně posílí bezpečnost, důvěru a konkurenceschopnost. Tyto cíle nejsou v rozporu, pokud EU zvolí risk-based, technologicky neutrální a prakticky proveditelný přístup.

Digital Council

Zdroje

[1] Evropská komise, „Targeted consultation on safeguarding the EU's data sovereignty", publikováno 8. července 2026; otevření konzultace 8. července 2026, uzavření 15. září 2026.

[2] Evropská komise, „Proposal for the Cloud and AI Development Act (CADA)", publikováno 3. června 2026; návrh je součástí širšího balíku k posílení evropského cloudového a AI ekosystému, investic a infrastruktury.

[3] Evropská komise, „Data Union Strategy – Unlocking Data for AI", 19. listopadu 2025; strategie vymezuje tři prioritní oblasti: rozšíření přístupu k datům pro AI, zjednodušení datových pravidel a posílení globální pozice EU v oblasti mezinárodních datových toků.

[4] Evropská komise, „Data Act explained"; Data Act se použije od 12. září 2025 a obsahuje záruky proti nezákonnému vládnímu přístupu třetích zemí k neosobním datům drženým v EU.

[5] Evropská komise, „Rules on international data transfers"; sada nástrojů GDPR pro předávání dat zahrnuje rozhodnutí o odpovídající ochraně, standardní smluvní doložky, závazná podniková pravidla, certifikační mechanismy, kodexy chování a výjimky.

[6] K vybraným příkladům pravidel a rámců ve třetích zemích viz Reserve Bank of India, „Storage of Payment System Data", 6. dubna 2018; turecký Úřad pro ochranu osobních údajů, oznámení ke standardním smlouvám pro přenosy do zahraničí; Uruguay URCDP Resolution No. 50/022 k modelovým smluvním doložkám a předchozímu povolení; Saudi Data and AI Authority, aktualizovaná regulace přenosů osobních údajů mimo Království; UAE Government, data protection laws; South African Government, National Data and Cloud Policy / kontext Public Procurement Act.

[7] Evropská komise, „Data Act explained", kapitola VI ke switchingu mezi službami zpracování dat; Data Act má umožnit zákazníkům hladce změnit poskytovatele a od 12. ledna 2027 ruší switching charges, včetně poplatků za odchozí přenos dat.

[8] Evropská komise, „Cloud and AI Development Act"; popis navrhovaných úrovní suverénních záruk zahrnuje požadavky týkající se zpracování v Unii, nezávislosti na třetích zemích, vlastnictví a kontroly v EU na úrovni 3 a možné uznání poskytovatelů ze třetích zemí.

[9] Eurostat, „53% EU enterprises used paid cloud services in 2025", 3. února 2026.

[10] OECD, „Cross-border data flows“; OECD popisuje Data Free Flow with Trust jako podporu volného toku dat při zajištění důvěry v oblasti soukromí, bezpečnosti a práv duševního vlastnictví a identifikuje rozhodnutí o odpovídající ochraně, mezivládní ujednání, obchodní dohody, standardy a privacy-enhancing technologies jako doplňkové nástroje. Global CBPR Forum, „About the Global CBPR Forum“; fórum spravuje systémy CBPR a PRP a usiluje o podporu ochrany dat a volného toku dat globálně.