

Digitální
a informační
agentura

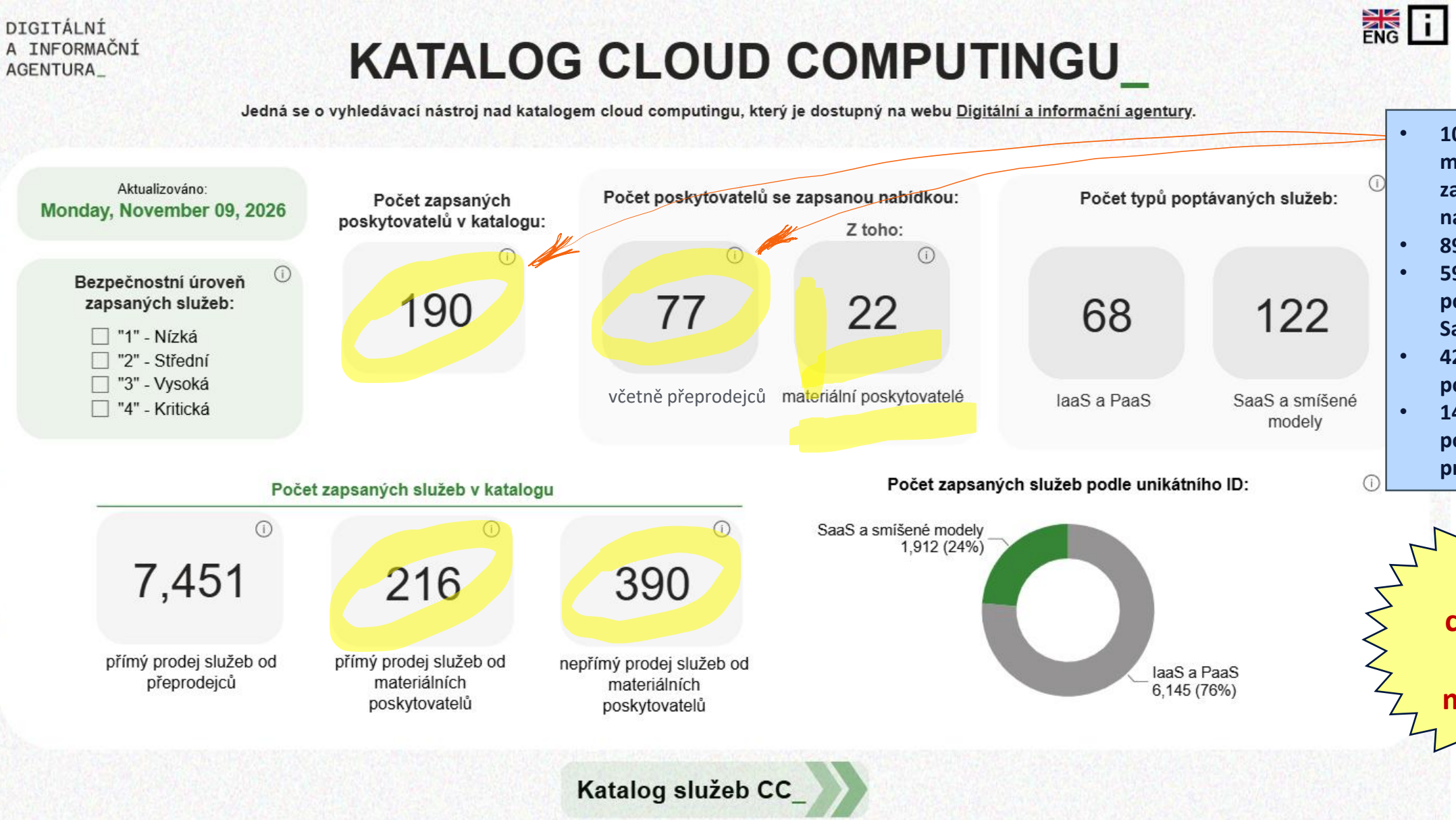
Kam směřují služby zapsané v Katalogu cloud computingu VS ….. a jak to souvisí s naší digitální suverenitou

Zdeněk Jiříček

Oddělení cloud computingu

Digitální a informační agentura

Katalog cloud computingu a cloudový ekosystém



- 100 prověřených místních společností, zatím bez registrované nabídky
- 89 z nich jsou MSP
- 59 z nich jsou potenciální vývojáři SaaS/PaaS
- 42 jsou integrátoři a potenciální reselleři
- 14 z nich jsou potenciální provozovatelé DC/IaaS

Potenciál cloudového trhu pro místní MSP!

eGovernment cloud – právní základ

Zákon o informačních systémech veřejné správy

Zákon č. 365/2000 Sb.

- Regulace cloud computingu je součástí zákona od roku 2021
- Vztahuje se na informační systémy podporující systematické informační činnosti pro veřejnou správu nebo jiné funkce státu
- Používají jej orgány veřejné správy (OVS)
- Úplný whitelist prostřednictvím katalogu cloud computingu

Zmocňuje a ukládá povinnosti

Vyhláška č. 411/2025 Sb.

Bezpečnostní úrovně ISVS

- Definuje 4 bezpečnostní úrovně IS (nízká, střední, vysoká, kritická)
- Vychází z úrovně dopadů v 8 oblastech dopadu

Přístup založený na dopadech

Vyhláška č. 505/2025 Sb.

Požadavky na zápis cloudových služeb do katalogu

- Stanoví bezpečnostní kritéria pro registraci CSP a jejich cloudových služeb v katalogu
- Kombinace kritérií kybernetické bezpečnosti a suverenity

Zajišťuje důvěryhodné cloudové služby ve veřejném sektoru

Vyhláška č. 412/2025 Sb.

Požadavky na OVS využívající cloud computing

- Stanoví bezpečnostní povinnosti **pro orgány veřejné správy** (PABs) využívající cloudové služby
- Definuje governance, řízení rizik a provozní požadavky

Podporuje bezpečné a odpovědné využívání cloudu OVS

Vyhláška č. 411/2025 Sb. o bezpečnostních úrovních (vytvořil NÚKIB)

Příloha

Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně

Oblasti dopadu								
	A.	**B.**	**C.**	**D.**	**E.**	**F.**	**G.**	**H.**
Úroveň dopadu	**Bezpečnost nebo zdraví lidí**	**Ochrana osobních údajů**	**Trestní řízení a páchání trestné činnosti**	**Veřejný pořádek**	**Mezinárodní vztahy**	**Důvěryhodnost orgánu veřejné správy**	**Finanční ztráty**	**Zajišťování služeb**
	Nemůže vést k poruše zdraví jednotlivce ani skupiny lidí.	Nemůže ovlivnit informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud	Nemůže vytvořit podmínky pro páchání trestných činů přisvojení pravomoci úřadu, zneužití	Nemůže zapříčinit hromadné nepokoje nebo jinak narušit veřejný pořádek.	Nemůže negativně ovlivnit obraz České republiky v zahraničí.	Nemůže negativně ovlivnit vztahy s jinými subjekty nebo vztahy s veřejností, nebo může vztahy s	Nemůže ani nepřímo vést k finančním ztrátám, nebo může vést k finančním ztrátám	Nemůže způsobit omezení, narušení nebo nedostupnost žádných poskytovaných služeb, nebo

Shrnutí bezpečnostních úrovní ISVS

Mimo oblast působnosti: utajované informace, bezpečnostní a zpravodajské služby, obrana a ozbrojené síly, Policie ČR, krizové řízení, trestní řízení, Česká národní banka a další.		→ Zpravidla on-premise, režimová prostředí
4. Kritická	**Kritická infrastruktura, narušení celostátního významu, >10 % rozpočtu OVS nebo >0,5 % HDP ČR, dopad na každodenní život >125 000 osob**	**Pouze poskytovatel cloud computingu ovládaný státem nebo určený vládou.** Data pouze v ČR, pokud OVS nepožádá jinak. (celkem 22 kritérií ve vyhl. č. 505/2025 Sb.)
3. Vysoká	**Narušení s dopadem na úrovni kraje, >5 % rozpočtu OVS nebo >0,1 % HDP ČR, dopad na každodenní život >50 000 osob**	**Komerční poskytovatel cloud computingu, ISO 27001/27017/27018 + zprávy SOC 2/ISAE/BSI C5; uložená data v EU, dočasné přenosy a bezpečnostní výjimky. Šifrování dat klíčem zákazníka.** (celkem 27 kritérií)
2. Střední	**Narušení s místním dopadem, >1 % rozpočtu OVS, dopad na každodenní život >5 000 osob**	**Poskytovatel cloud computingu: ISO 27001 a 27017, transparentnost umístění dat.** (celkem 15 kritérií)
1. Nízká	**Bez dopadu na veřejný pořádek, např. informační weby nebo turistický portál**	**Vlastní posouzení poskytovatele, transparentnost umístění dat** (celkem 14 kritérií)

Principy prověřování poskytovatelů podle ZoISVS

Dvouúrovňová kvalifikace: zákonná důvěryhodnost a podrobné prováděcí požadavky

HLAVNÍ ZÁKON | způsobilost a důvěryhodnost

1. **Ochrana C-I-A** — Schopnost zajistit základní úroveň důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy.
2. **Bezúhon-nost** — Splňuje zákonné požadavky na bezúhonnost správce kvalifikovaného systému elektronické identifikace podle českého práva.
3. **Způsobilost** — Je způsobilý poskytovat cloud computing orgánům veřejné správy s ohledem na veřejný pořádek, bezpečnost a práva třetích osob.

PROCES PROVĚŘENÍ

Až 3 měsíce

Kontroly konečných vlastníků, AML, bezpečnostních a zpravodajských služeb

PROVÁDĚCÍ VYHLÁŠKA | provozní záruky

- **Přítomnost v EU** — Sídlo v EU/ESVO (případně ustanovený zástupce).
- **Kybernetická historie** — Poskytovatel ani jej ovládající osoby nebyli v posledních pěti letech pravomocně odsouzeni za relevantní trestný čin v oblasti kybernetické bezpečnosti.
- **Umístění dat** — Požadavky na ukládání a zpracování zákaznických dat a osobních provozních údajů v EU/ESVO (včetně výjimek).
- **Požadavky zahraničních orgánů** — Dokumentovaný postup pro vyřizování žádostí zahraničních orgánů o přístup k chráněným datům nebo jejich předání.
- **Právní expozice** — Uvedení použitelných právních předpisů států mimo EU/EHP, které mohou vynutit přístup k těmto datům nebo jejich předání.

Prověření určuje, zda může být poskytovatel zapsán do katalogu cloud computingu.

Stávající česká kritéria suverenity (co zahrnují)

Český rámec eGovernment cloudu již uplatňuje přiměřené záruky suverenity prostřednictvím modelu založeného na riziku a dopadu.

Všechny bezpečnostní úrovně

- **Zavedené postupy chrání data OVS před neoprávněným nebo nepřiměřeným zpřístupněním.**
- **Pro hodnocení rizik se vyžaduje transparentnost umístění dat a vzdálené administrace cloudu.**

Bezpečnostní úroveň 3 – vysoká

- **Komerční poskytovatelé, pokud splní kvalifikační kritéria.**
- Musí **umožnit šifrování** dat v cloudu klíči ve **výhradní správě** OVS.
- Musí **využít veškeré právní nástroje**, aby zabránil zpřístupnění dat zahraničnímu orgánu bez souhlasu OVS.

Bezpečnostní úroveň 4 – kritická

- **Státní poskytovatel,** který není přímo vystaven exteritoriálním požadavkům na zákaznická data.
- **Nejpřísnější režim suverenity** pro informační systémy s kritickou úrovní dopadů dle vyhl. č. 411/2025 Sb.

CSP: POVINNÁ TRANSPARENTNOST

Zpracování dat

CSP musí uvést státy trvalého uložení a dočasného zpracování dat.

Správa cloudu

CSP musí uvést státy, z nichž se provádí správa a monitorování cloud computingu.

Zpracování mimo EU/EFTA

Rozsah, doba, účel a místo zpracování musí být dokumentovány; výjimky pro dlouhodobé uložení mimo EU/ESVO u úrovně 3 se zveřejňují.

POVINNOST OVS

Na základě rizika: posoudit riziko přístupu třetích stran nebo přerušení cloudové služby a využívat pouze takové služby cloud computingu, jejichž rizika pro bezpečnost informací jsou přijatelná.

Česká regulace již kombinuje suverenitu, transparentnost, šifrování a akceptaci rizik.

Legal basis: Zákon č. 365/2000 Sb.; Decrees No. 505/2025 Sb. a No. 412/2025 Sb. | PAB = Public Administration Body

Řízení rizik poskytovatelů regul. služeb dle nZKB

V režimu vyšších povinností

1. **Aktiva**
2. **Hrozby & zranitel-nosti**
3. **Posouzení rizik**
4. **Mitigace a zvládání rizik**
5. **Přezkum po 12 měsících**

- OVS si může zvolit metodiku řízení rizik v mezích právního rámce
- § 15 nZKB: **politika kontinuity činností;** příloha č. 3 zahrnuje **geopolitické hrozby;** příloha č. 5 rizika **dodavatelského řetězce**

V režimu nižších povinností

Přiměřená bezpečnostní opatření

Prováděcí vyhláška stanoví minimální soubor bezpečnostních opatření, přičemž celkový způsob jejich zavedení zůstává přiměřený rizikovému profilu regulovaného subjektu.

Minimální základ + přiměřené zavedení

VYHLÁŠKA Č. 412/2025 SB. | požadavky na OVS využívající cloud computing

RIZIKO PŘÍSTUPU ZAHRANIČNÍCH ORGÁNŮ

Posoudit a dokumentovat rizika vyplývající z umístění dat, včetně přístupu nebo zpřístupnění na základě požadavku zahraničního orgánu. Službu využít pouze tehdy, je-li riziko přijatelné.

ZÁKLADNÍ OPATŘENÍ

14 oblastí základních bezpečnostních opatření, včetně BC/DR plánu, Exit plánu a šifrování dat…

Návrh EU nařízení CADA

Cloud and AI Development Act (publikováno 06/2026, předpoklad účinnost za 2 – 3 roky)
V procesu připomínkování: gestor MPO, spolugestor DIA, dále NÚKIB, MV, MZV, MMR

CÍL Část „AUTONOMY“: Posílit digitální suverenitu cloudových služeb využívaných veřejnou správou a subjekty vykonávajícími kritické nebo strategicky významné činnosti.

PŘÍSTUP ZALOŽENÝ NA RIZIKU

- Členské státy **posoudí rizika svých činností a zařadí je do úrovní UAL 1 až UAL 4.**
- Metodika pro vyhodnocení rizik pro UAL má být **jednotná v rámci EU**
- **Dodatečné geopolitické/netechnické požadavky** nad rámec NIS2, CRA, CER, EU Data Act, EU AI Act
- **Omezení CSP pod kontrolou třetích zemí** od v UAL 2 až 4 (risk-based)

UZNÁVÁNÍ CLOUDOVÝCH SLUŽEB

- Poskytovatelé cloud computingu (CSP) v celé EU a jejich služby projdou **procesem uznání pro příslušnou úroveň UAL 1 až UAL 4**.
- Veřejní zadavatelé budou pro vymezené činnosti **poptávat pouze služby uznané pro odpovídající úroveň UAL.**

ANNEX II A III

SUVERENITNÍ POŽADAVKY, CLOUD & SW SUPPLY CHAIN

1. **Kritéria pro Union Assurance Levels**
   Požadavky na poskytovatele cloud computingu pro jednotlivé úrovně autonomie.
2. **Seznam auditních požadavků**
   Prověřování vlivu a závislostí na třetích zemích podle úrovní UAL 1 - 4
3. **Self-assessment vs. auditní zpráva**
   V návrhu je:
   UAL 1 – Self-assessment
   UAL 2 – 4: Nezávislá auditní zpráva

https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada

Exteritoriální přístup orgánů činných v trestním řízení – USA vs. EU

USA i EU zavádí přístup zrychlených žádostí OČTŘ na poskytovatele, který má data v držení nebo pod kontrolou, bez ohledu na umístění dat

USA: Stored Communications Act / CLOUD Act

Účel	Trestní vyšetřování a elektronické důkazy
Působnost	Poskytovatel podléhající jurisdikci USA (pobočky, významné obchodní aktivity, cílené poskytování služeb v USA); **umístění dat není rozhodující**
Omezení	Možnost namítat střet se zahraničním právem
Autorizace	**Kontaktní údaje: Subpoena** (předvolání) **Provozní logy: Court order** (soudní příkaz) **Obsah komunikace: Warrant** (soudní povolení k prohlídce)

EU: nařízení e-Evidence (EU) 2023/1543

Účel	Přeshraniční elektronické důkazy v trestním řízení
Působnost	Služba nabízena v EU prostřednictvím provozovny nebo určené osoby v EU; **umístění dat není rozhodující**
Omezení	Evropský vydávací příkaz **proti orgánu veřejné moci** lze uplatnit pouze **vůči orgánům vydávajícího členského státu**.
Autorizace	**Státní zástupce pro kontaktní údaje.** **Soud pro obsah a většinu provozních údajů**

Právní, organizační a technické oddělení provozu v EU může omezit přístup třetích zemí

KOMPROMIS

Plné oddělení může zabránit vykonat evropský vydávací příkaz, jsou-li požadovaná data mimo EU.

Žádosti OČTŘ za r. 2025

Požadavky vedoucí k alespoň částečnému zpřístupnění jsou uvedeny v závorkách

SVĚT		EU-27		NĚMECKO		FRANCIE		ČESKO	
Microsoft	Google	Microsoft	Google	Microsoft	Google	Microsoft	Google	Microsoft	Google
58,042 (37,717)	591,929 (~493,478)	21,261 (12,935)	173,240 (~145,742)	8,556 (4,948)	88,678 (~76,704)	3,989 (2,227)	18,896 (~15,289)	36 (27)	920 (~872)

Microsoft uvádí za r. 2025 jen 190 žádostí na data firemních zákazníků globálně, z toho byla vydána jen ve 3 případech mimo USA a z toho 1 se nacházel v EU/ESVO

Digitální a informační agentura

Rozsah: Microsoft, žádosti v trestních věcech a naléhavé žádosti; Google, žádosti o zpřístupnění bez žádostí pouze o uchování dat. Počty zpřístupnění u Googlu jsou odhadem z publikovaných zaokrouhlených procent.

Rizika pro důvěrnost dat:

Datová rezidence vs. šifrování výhradně pod kontrolou zákazníka

ZÁKONNÉ ZPŘÍSTUPNĚNÍ DAT CSP

- **Poskytovatel mající business i mimo EU** může splnit příkaz k vydání dat, který považuje za zákonný a závazný podle práva třetí země.
- Vyšetřování závažné přeshraniční trestné činnosti nemůže dlouho čekat (postupy MLAT).
- Samotné fyzické umístění dat nemusí zpřístupnění zabránit.

CSP MŮŽE PODLÉHAT JURISDIKCI MIMO EU

- Canada v. OVHcloud: zahraniční soud může potvrdit přímý příkaz k vydání dat vůči poskytovateli s dostatečnou místní přítomností.
- Ukládání pouze v EU a sídlo v EU jsou právní a organizační záruky, nikoli absolutní technická překážka.

ŠIFROVÁNÍ VÝHRADNĚ POD KONTROLOU ZÁKAZNÍKA

- CSP může nakonec vydat jen metadata a maximálně šifrovaný obsah.
- Rozhodující je technická nedostupnost šifrovacího klíče pro poskytovatele.

POŽADAVEK ČESKÉ REGULACE

- Úrovně 3 a 4 vyžadují možnost šifrování obsahu pod kontrolou zákazníka; **úroveň 4 navíc požaduje ochranu certifikovaným HSM.**
- **Vyžadují se schválené algoritmy (kritérium 5.3); požadavky na kontrolu klíčů stanoví kritérium 5.4.**

KRYPTOGRAFICKÝ ÚČINEK

- Šifrování cloudových dat obvykle používá silnou symetrickou kryptografii; **AES-256 si zachovává vysokou bezpečnostní rezervu i vůči předvídatelným kvantovým vyhledávacím útokům.**
- **Chrání to obsah, nikoli však provozní, účastnická ani jiná metadata.**

ZÁVĚR HODNOCENÍ RIZIK

Umístění dat a založení společnosti v EU snižují jurisdikční expozici. Šifrování pod výhradní kontrolou zákazníka může být silnější zárukou důvěrnosti, protože poskytovatel může mít zákonnou povinnost reagovat, ale nebude schopen zpřístupnit srozumitelný zákaznický obsah.

Rizika pro dostupnost a integritu dat

BEZPEČNOSTNÍ ÚROVEŇ 3 – Vysoká

- Zákaznická data a specifické provozní údaje v EU
- SLA a smluvní záruky dostupnosti služeb a dat

Volba suverenity založená na riziku

Cloud supply chain: Vždy existuje riziko sankcí, embarga, duálního využití technologií, které je nutné zvážit.

CSA2 (připravuje se): Trusted ICT Supply chain framework, „High-risk suppliers“, non-technical risks

CRA nařízení: povinnosti pro „produkt s digitálními prvky“; řízení zranitelností, netechnická rizika dodavatelů.

BEZPEČNOSTNÍ ÚROVEŇ 4 – KRITICKÁ

- Pouze státní poskytovatel
- Uložení a zpracování dat v ČR;
  Přenosy mimo ČR pouze s výslovným souhlasem OVS

DOSTUPNOST: PŘÍSTUP ZALOŽENÝ NA RIZIKU

1 – ZPRACOVÁNÍ DAT V EU	• Infrastruktura datových center v EU, regiony volené zákazníkem • Uložení a zpracování dat v EU (kromě výjimek)
2 - DODATEČNÉ SMLUVNÍ ZÁRUKY	• Pro zákazníky z veřejné správy závazek: • **Právně napadat kolidující nebo nepřiměřené příkazy** na vydání dat včetně vynuceného omezení služby
3 – SUVERENITA PROVOZU SLUŽEB	• **Žádné subdodávky cloud. služeb** ze zemí mimo EU • Provoz a podpora jen osobami usazenými v EU • **Žádný přístup k zákaznickému obsahu mimo EU** • Omezený a kontrolovaný **přístup ze třetích zemí ke Control plane a Service generated data** poskytovatele
4 - ODDĚLENÝ SUVERÉNNÍ CLOUD	• **HQ/vlastník i mimo EU, a řízení v EU** • Oddělená infrastruktura DC včetně Control Plane v EU • **Mimo přímé držení, úschovu nebo kontrolu mateřské společnosti v USA (dle CLOUD Act)**
5 - NEZÁVISLÝ PARTNERSKÝ CLOUD V EU	• Bez vlastnictví mateřskou společností ze třetí země • Může vyžadovat, **aby poskytovatel z EU neměl obchodní zájmy ve třetích zemích** (viz případ Canada vs. OVHcloud).

Suverenita není binární, ale risk-based

Suverenita je flexibilita ve výběru a rozhodování

Suverenita je schopnost využívat nejlepší dostupné technologie, aniž bychom se stali závislými na konkrétním dodavateli, platformě nebo jurisdikci.



Digitální
a informační
agentura

Dotazy

Zdeněk Jiříček

Oddělení cloud computingu

Digitální a informační agentura

zdenek.jiricek@dia.gov.cz