SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

V PRAZE DNE 24. BŘEZNA 2016
Č.J.: GŘ/25/SMV

Stanovisko Svazu průmyslu a dopravy ČR
k materiálu Ministerstva vnitra ČR
Národní strategie cloud computingu

Obecné připomínky:

1. **Obecná připomínka:**

Svaz průmyslu a dopravy ČR (dále jen „SP ČR“) doporučuje pozastavit projednávání návrhu a předložit k projednání vládě materiál užšího rozsahu, který bude obsahovat informaci o tom, že záměrem vlády, resp. předkladatele materiálu je zřídit státní cloud, vymezí systémy, na které se bude při užití státního cloudu vztahovat pravidlo „cloud only“, bude deklarovat záměr nekonkurence mezi státním cloudem a soukromými cloudovými úložišti při respektování principů ochrany trhu a reflexi postupného vývoje souvisejícího s postupným opouštěním separátních cloudových úložišť. Zdůrazňujeme, že při zřízení státního cloudu je třeba hledat právní základ pro jeho fungování tak, aby byl zachován základní princip veřejného práva v případě *a silentio legis* – tedy že veřejnou moc lze uplatňovat pouze v případech explicitně zákonem upravených.

SP ČR je pak připraven k aktivní spolupráci s předkladatelem na předložení nové širší verze materiálu, který vymezí bližší podmínky fungování státního cloudu, fáze jeho zavádění a další související otázky tak, aby zahájení jeho činnosti bylo co nejrychlejší a nejefektivnější.

Odůvodnění:

SP ČR podporuje snahu státu nastavit efektivní, účinný a transparentní systém řízení ICT veřejné správy (i včetně zavedení eGOV cloud computingu pro správu legislativou definovaných kritických dat a kritické infrastruktury). Zároveň podporujeme snahu státu snížit administrativní zátěž občanů a podnikatelů prostřednictvím realizace další etapy eGovernmentu, jakou by mělo být dokončení státního datového fondu, sdílení jednou získaných dat, zjednodušení přístupu občanů k veřejné správě, optimalizace a standardizace výkonu agend veřejné správy. Na základě výše uvedeného proto SP ČR podporuje takové návrhy, které budou směřovat k naplnění stanovených cílů a přitom budou respektovat nejen ústavní principy demokratické společnosti (volné tržní prostředí, ochrana soukromého vlastnictví, rovná hospodářská soutěž, výkon veřejné správy jen v rozsahu a za podmínek definovaných právním řádem ČR, apod.), ale také právní úpravu dané oblasti (veřejná podpora, služby v obecném a obecném hospodářském zájmu, apod.), včetně úpravy unijní.

Předložený návrh však výše uvedené parametry nesplňuje výše uvedené parametry, neřeší

TELEFON (+420) 225 279 111 | 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.

komplexně a koncepčně danou oblast, vychází z nepodložených závěrů, a proto jej z dále uvedených důvodů nelze v předložené podobě doporučit vládě ke schválení. Po dopracování návrhu dle dále uvedených připomínek, které jsou příkladem námitek soukromého sektoru vůči předloženému materiálu, by však bylo zřejmě možné v úzké spolupráci s odborným sektorem postupnými kroky stanoveného cíle sátu dosáhnout.

Tato připomínka je zásadní.

Konkrétní připomínky k jednotlivým částem materiálu:

2. **Připomínka ke Kapitole 1 Manažerské shrnutí:**

Navrhujeme text upravit takto (doplněné/změněné části jsou podtrženy):

Strategie je vedena snahou vybalancovat využití státního a komerčního cloudu tak, aby stát měl pod kontrolou ty ICT služby nebo data, která mají pro stát strategický význam, zejména z důvodů bezpečnosti nebo utajení, a současně aby pro ostatní ICT služby maximálně využil tlaku tržního prostředí na cenu služeb.

Klíčovým opatřením, které je zaměřeno na nové aplikace/ICT služby je soubor pravidel, jak budou nové ICT služby opatřovány. ***Bude-li OVM požadovat novou ICT službu, pak:***

- *je-li tato služba nabízena státním cloudem, musí být použita (avšak s vymezením působnosti státního cloudu jak je uvedeno dále v této Strategii),*
- *je-li tato služba nabízena komerčním cloudem, pak platí princip „cloud first" – viz kap. 5,*

není-li daná služba nabízena ani státním ani komerčním cloudem (bude se jednat nejspíše o aplikaci s novou specializovanou funkčností), pak bude aplikace pořízena mimo eGovernment cloudu, ale provozována musí být v rámci eGovernment cloudu. Při volbě cloudové platformy (IaaS / PaaS) ze státního nebo komerčního cloudu bude přihlédnuto k Základním principům eGC viz kap. 5 odst. d).

Odůvodnění:

V rámci souboru pravidel pro opatřování nových ICT služeb (str. 5) se v materiálu uvádí, že bude-li OVM požadovat novou ICT službu, pak je-li tato služba nabízena státním cloudem, musí být použita (stejně tak je uvedeno i v kapitole 8.4) Z toho však vyplývá, že by všechny OVM musely vždy služby nakupovat ve státním cloudu, pokud by tam byly nabízeny, a to i tehdy, pokud by pro to nebyly důvody bezpečnostní nebo utajení (viz definice v kapitole 5 písm. e), a v cloudu komerčním by tytéž služby byly ekonomicky výhodnější, tj. s nižšími TCO.
To je dále v rozporu s obrázkem 1 „Struktura eGovernment cloudu" na str. 14, ze kterého plyne, že některé služby mohou být poskytovány jak státním, tak komerčním cloudem.

Doporučujeme zpřesnění a sjednocení textu tak, aby bylo zřejmé, zda OVM musí automaticky služby nakupovat ve státním cloudu (i když by pro to nebyly žádné důvody bezpečnostní nebo utajení) a v komerčním cloudu by tyto služby byly ekonomicky výhodnější, tj. s nižšími TCO).

3. **Připomínka ke Kapitole 1, poslední odstavec str. 5, a dále ke Kapitole 5, písm. e), str. 12:**

Navrhujeme text upravit takto (doplněné/změněné části jsou podtrženy):

Ve státním cloudu budou provozovány zejména ty ICT služby a data, které splňují některou z

následujících podmínek:

- *Jde o aplikace, případně jejich funkční části nebo data, která mají pro stát strategický význam zejména z důvodů bezpečnosti nebo utajení.*
- *Mají jedinečnou funkcionalitu, která není standardně nabízena na trhu, je nezbytná jejich standardizace pro všechny uživatele VS a zároveň mají strategický význam pro stát.*

Požadavek na umístění takových ICT služeb a dat ve státním cloudu odůvodněně vyplyne z výsledku analýzy rizik a z příslušné kategorie hodnocení aktiv podle Zákona o kybernetické bezpečnosti a jeho prováděcí vyhlášky č. 316/2014 Sb. Kde taková situace nenastane, budou tyto systémy (včetně systémů VIS a případně i KII ve smyslu ZoKB) moci být provozovány částečně nebo i úplně v komerčním cloudu.

Odůvodnění:

Podmínky pro provoz aplikací ve státním cloudu v kapitole 1 jsou definovány velmi obecně (zahrnující plošně většinu aplikací používaných ve veřejném sektoru) a nejednotně, tj. odlišně než základní principy v kapitole 5 (písm. e) na str. 12

Doporučujeme sjednotit definice uvedené v materiálu tak, aby bylo zřejmé, co musí splňovat dané aplikace pro to, aby mohly být umístěny výlučně ve státním cloudu a za jakých podmínek mohou být umístěny v komerčním cloudu.

Reference k Zákonu o kybernetické bezpečnosti – Ve vymezení podmínek pro provoz aplikací ve státním cloudu v kapitole 1 na straně 6 je uvedena podmínka (poslední bod), že ve státním cloudu budou provozovány aplikace, které jsou pod působností zákona o kybernetické bezpečnosti v kategorii VIS nebo KII.

Zákon nicméně nestanovuje podmínku, že aplikace v kategorii VIS nebo KII nemohou být provozovány v jiném než státem vlastněném datovém centru.

Zároveň ZKB prostřednictvím vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ponechává prostor správcům IS, aby sami stanovili, jaké aplikace spadají do kategorie VIS. Domníváme se, že toto vymezení podmínek pro provoz aplikací ve státním cloudu je neodůvodněně široké, a není dostatečné a srozumitelné z hlediska ostatních služeb, které mohou být poskytovány jak státním, tak komerčním cloudem.

Navrhujeme: upřesnit definici aplikací, které musí být umístěny ve státním cloudu a nelze je umístit do komerčního cloudu, i kdyby to bylo ekonomicky výhodnější, a to včetně konkrétního vymezení parametrů, které by taková aplikace musela splňovat.

4. Připomínka ke Kapitole 5 (základní principy eGC), str. 12:

Navrhujeme text upravit takto (doplněné/změněné části jsou podtrženy):

d) Sdílené ICT služby – mezi aktuálně provozovanými infrastrukturními, platformními a aplikačními ICT službami VS budou identifikovány kategorie funkčně podobných ICT služeb, u kterých budou stanoveny minimální standardy bezpečnosti a interoperability. V případě služeb různých dodavatelů bude postupně zajištěna možnost migrace (přenositelnosti) dat při zachování principu dlouhodobého fungování tržního prostředí. Tím dojde k postupnému snížení celkového počtu vyhovujících aplikací od různých poskytovatelů, v souladu s fungováním rámců nabídek komerčního cloudu (jak je popsáno dále).

Odůvodnění:

Souhlasíme s tím, že je nutné zajistit minimální úroveň standardizace u funkčně podobných nebo zákonem daných aplikací nebo služeb od různých dodavatelů, což je žádoucí podmínkou zefektivnění provozu těchto aplikací a snížení rizika „lock-in". Současně je však třeba zachovat konkurenční prostředí u takových aplikací a služeb, které se nebudou pořizovat prostřednictvím jediného OVM pro celou veřejnou správu.
Pokud tedy daná aplikace bude splňovat minimální funkční požadavky a standardy bezpečnosti a interoperability, potom jednotlivé ISVS pořizované od různých dodavatelů mohou zůstat zachovány v rámci tržního prostředí komerčního cloudu. Např. spisová služba nebo elektronická úřední deska, jejíž funkčnost je stanovena zákonem, by měla zůstat v rámci zachování efektivního tržního prostředí dostupná od různých dodavatelů. Bude tedy třeba rozlišit mezi situací, kdy již existuje trh pro danou aplikaci a kdy bude proto z dlouhodobého pohledu vhodné tento relevantní trh i nadále zachovat funkční.

5. **Připomínka ke Kapitole 5 (základní principy eGC), str. 12:**

Navrhujeme text upravit takto (doplněné/změněné části jsou podtrženy):

e) eGovernment cloud (eGC) bude tvořen státními datovými centry (státní cloud) a komerčními datovými centry (komerční cloud). Ve státním cloudu budou provozovány ty ICT služby, jejichž provozování privátními subjekty není z důvodů bezpečnosti nebo utajení možné.

Požadavek na umístění ICT služeb a dat ve státním cloudu odůvodněně vyplyne z výsledku analýzy rizik a z příslušné kategorie hodnocení aktiv podle Zákona o kybernetické bezpečnosti a jeho prováděcí vyhlášky č. 316/2014 Sb. v tom smyslu, že výsledná rizika a požadavky na zabezpečení dat dle Vyhlášky nebude možné zajistit v komerčním cloudu. Státní cloud se bude vyznačovat vysokými požadavky na zabezpečení, jako jsou:

- *Odolnost proti výpadkům na úrovni minimálně Tier III (Uptime Institute)*
- *Certifikace bezpečnosti služeb dle ISO 27001, ochrany soukromí dle ISO 27018, a řízení rizik dle ISO 27005*
- *Personální bezpečnost- všichni administrátoři ve státním cloudu s jakoukoli možností přístupu na data nebo poskytované ICT služby budou muset získat „osvědčení personální bezpečnosti" pro fyzické osoby minimálně stupně „Tajné".*

Všechny ostatní služby mohou být poskytovány jak státním cloudem, tak komerčním cloudem tak, aby vznikl tlak na snižování cen ICT služeb.

Odůvodnění:

Doporučujeme uvést specifické požadavky na bezpečnost ve státním cloudu, které by měly být s ohledem na charakter provozovaných ICT služeb (strategický význam pro stát z důvodů bezpečnosti nebo utajení) vyšší než u komerčních provozovatelů cloudových služeb. Viz dále Kap. 6 obr. 1, kde je zřejmé rozdělení: Státní cloud = vysoce bezpečné služby, Komerční cloud = nízko a středně bezpečné služby.

6. **Připomínka k Kapitole 6 Struktura eGC, obr. 1, str. 14:**

Navrhujeme změnit Obr. 1 tak, aby i Agendové systémy umožňovaly nasazení v komerčním cloudu dle konkrétních požadavků na bezpečnost a utajení.

Odůvodnění:

Není zřejmé, z jakého důvodu by všechny Agendové systémy měly být poskytovány pouze ze státního cloudu, v „zóně vysoce bezpečných služeb“, jejichž provoz bude velmi pravděpodobně dražší než provoz v tržním prostředí komerčního cloudu. Je třeba zohlednit možná rizika a konkrétní požadavky na důvěrnost a integritu dat a dostupnost dané služby, a jestliže příslušný agendový systém nespadne do vymezení „státního cloudu“, není důvod uplatňovat horizontální „in house“ výjimku.

7. **Připomínka ke Kapitole 6 Struktura eGC, str. 15:**

Viz návrh formulace v Připomínce č. 3.

Odůvodnění:

Navrhujeme sjednotit vymezení státního cloudu s upravenou formulací pro manažerské shrnutí.
Dále bude důležité určit, jakou formou budou specifikovány ICT služby a data, které musejí být provozovány pouze ve státním cloudu, tj. zda např. formou taxativního výčtu, či formou konkrétních závazných pravidel, ze kterých by vyplývala omezení pro umístění ICT služeb (respektive dat) do komerčního cloudu – např. na základě analýzy rizik a hodnocení aktiv dle VoKB č. 316/2014 Sb, jak je uvedeno v Připomínce č. 3.

8. **Připomínka ke Kapitole 7, část 7.1.1, str. 16 nahoře, a dále i Kapitole 8, část 8.1.1, str. 20:**

Navrhujeme text upravit takto:

Státní cloud bude od roku 2017 tvořen nejméně dvěma geograficky oddělenými datovými centry, *které budou umožňovat vůči sobě provoz aplikací a správu dat s možností obnovy provozu (Disaster Recovery). Vzhledem k vysokým počátečním investicím nutným k zajištění vysoké úrovně garantované dostupnosti (min. 99,9%) a odolnosti proti výpadkům použít metodiku TCO tak, aby nedošlo k poddimenzování kapacity, nebo naopak ke zbytečně vynaloženým nákladům z veřejných rozpočtů.*

Dále bude vhodné umožnit scénář Disaster Recovery i zálohováním dat a služeb v komerčním cloudu ve vzdálenějších lokalitách za účelem mitigace ***(snížení)*** *strategických, environmentálních, a geopolitických rizik.*

Odůvodnění:

Doporučujeme blíže specifikovat, na základě jakých kritérií se bude rozhodovat o počtu a kapacitě datových center státu

a zda k tomuto účelu bude využita metodika TCO tak, aby nedošlo k poddimenzování kapacity, nebo naopak ke zbytečně vynaloženým nákladům z veřejných rozpočtů. Je známo, že v případě Slovenské republiky jsou plánované náklady na výstavbu 2 moderních státních datových center ve výši 250 mil EUR, tedy cca 6,75 miliard Kč. Je otázkou, zda tak vysoká počáteční investice plus další provozní náklady jsou odůvodnitelné ve srovnání s komerčním cloudem, kde zákazníci veřejné správy platí

pouze průběžné náklady za to co spotřebují, a to v tržním cenovém prostředí.

Doporučujeme dále zohlednit scénáře Disaster Recovery (D/R), kdy některé ICT služby mohou být zálohovány do komerčního cloudu pro případ havárie. Použití pouze dvou až tří státních datových center na území hl. m. Prahy ve vzdálenosti několika kilometrů není z hlediska strategických, environmentálních, a geopolitických rizik nejlepší volbou

9. **Připomínka ke Kapitole 7, část 7.1.1, str. 16 uprostřed:**

   Navrhujeme text přeformulovat.

   Odůvodnění:

   Existuje obava, že po letošní novele ZVZ (duben 2016) nelze očekávat průchod další novely ZVZ po další cca 3 roky. Navrhujeme proto prozkoumat, jak by bylo možné využít pro nákup cloudových služeb stávajících institutů ZVZ, zejména institutu rámcových smluv.

10. **Připomínka ke Kapitole 8, část 8.1.1:**

    Viz návrh změny textu ke kap. 7.1.1.

    Odůvodnění:

    Doporučujeme blíže specifikovat principy „cloud only", „cloud first" a „dobrovolné využití" z hlediska navrhované právní úpravy zadávání veřejných zakázek a z hlediska navrhované metodiky TCO.

11. **Připomínka ke Kapitole 8, část 8.1.1, str. 21 nahoře:**

    Navrhujeme text upravit takto (doplněné/změněné části jsou podtrženy):

    *…pro přechod do **komerčního cloudu** bude užit princip „**cloud first**", tj. při nákupu nové služby nebo při obnově stávající služby se musí využít služba nabízená v komerčním cloudu, když jsou současně splněny tyto podmínky:*

- *odpovídající služba je v komerčním cloudu nabízena,*
- *TCO nabízené služby v komerčním cloudu je nižší, než TCO služby pořízené a provozované mimo komerční cloud.*

  Stávající metodiku TCO bude nutné doplnit tak, aby lépe korespondovala se skutečným stavem, tedy doplnit o kvalifikované odhady nákladovosti pro případy, kdy subjekty veřejné správy nedokážou jednoduchým způsobem požadované vstupy do TCO kalkulace zajistit.

  Odůvodnění:

  Klíčové je stanovení realistické metodiky TCO, která nastaví takové parametry výpočtu, jež zohlední skutečné náklady provozu při srovnatelných podmínkách dostupnosti a zabezpečení. Současná verze metodiky TCO neobsahuje všechny relevantní náklady. Existuje riziko, že výpočty TCO pro rozhodnutí ohledně umístění aplikací nebudou navzájem porovnatelné z důvodu nezahrnutí části nákladů do kalkulací jednotlivých nabídek. Doporučujeme zahrnutí všech relevantních nákladů do metodiky TCO.

12. <u>Připomínka ke Kapitole 9, str. 25:</u>

Navrhujeme text přeformulovat ve smyslu odůvodnění níže.

<u>Odůvodnění:</u>

Doporučujeme konkrétněji specifikovat pravomoci Certifikačního orgánu (CO), Odboru hlavního architekta (OHA) eGovernmentu a RVIS, aby byla více zřejmá hierarchie rozhodovacích pravomocí pro účely eGC.
Dále považujeme za nezbytné blíže specifikovat, jak by měla být legislativně ukotvena činnost CO a OHA (mj. v rámci novelizace zákona o ISVS), a to zejména v návaznosti na závažnost kompetencí, s nimiž NSCC počítá (určování závazných pravidel pro ostatní instituce VS).
Dále Doporučujeme sjednotit v celém dokumentu vymezení kompetencí jednotlivých složek vůči eGC. Pravomoci Certifikačního orgánu, Odboru hlavního architekta eGovernmentu a RVIS při určení služeb, které mohou být provozovány v jednotlivých částech eGC (státní, komerční cloud), nejsou promítnuty nikde v předchozím textu, který se uvedeným vymezením zabývá (zejména kapitoly 5 a 6).

13. <u>Připomínka ke Kapitole 9, část 9.2 Financování státního cloudu:</u>

Navrhujeme text přeformulovat takto:

V případě, že by při počáteční investici nebo provozu státního cloudu byly využity evropské fondy, je nutné zamezit dvojímu financování ze strany klientských organizací (tzn. že státní datové centrum své služby OVM nesmí účtovat). <u>Proto by bylo důležité</u>

<u>zpřesnit podmínky pro dotované financování tak, aby nekonkurovalo nabídkám privátních poskytovatelů v komerčním cloudu splněním následujících podmínek:</u>

- *<u>V rámci přípravy (a následně hodnocení, např. ze strany OHA) projektů zohlednit, jakým způsobem je zajištěno financování provozní fáze a fáze udržitelnosti.</u>*
- *<u>Součástí hodnocení projektu by mělo být ekonomické hodnocení (studie proveditelnosti, CBA), které bude obsahovat analýzu předpokládaných nákladů a výnosů, a to jak v provozní fázi, tak ve fázi udržitelnosti projektu.</u>*
- *<u>Zároveň by mělo ekonomické hodnocení projektu vycházet z reálného odhadu naplnění kapacity DC.</u>*
- *<u>V rámci ekonomického posouzení projektu před jeho financováním z ESIF (tj. studie proveditelnosti, CBA) je nezbytné odůvodnit výši provozních výdajů z veřejných rozpočtů na zajištění udržitelnosti projektu.</u>*

<u>Je třeba posoudit již v přípravné fázi, zda se v případě cloudových služeb poskytovaných v rámci eGC bude jednat o služby obecné nehospodářské povahy (angl. Service of General Non-Economic Interest, SGNEI) nebo služby obecného hospodářského zájmu (SGEI). Tímto postupem bude minimalizováno riziko nedovolené státní podpory při budování datových center z veřejných zdrojů (respektive ESIF).</u>

<u>Odůvodnění:</u>

Doporučujeme konkrétněji specifikovat pravomoci Certifikačního orgánu (CO), Odboru hlavního

architekta (OHA) eGovernmentu a RVIS, aby byla více zřejmá hierarchie rozhodovacích pravomocí pro účely eGC.

Dále považujeme za nezbytné blíže specifikovat, jak by měla být legislativně ukotvena činnost CO a OHA (mj. v rámci novelizace zákona o ISVS), a to zejména v návaznosti na závažnost kompetencí, s nimiž NSCC počítá (určování závazných pravidel pro ostatní instituce VS).

Dále Doporučujeme sjednotit v celém dokumentu vymezení kompetencí jednotlivých složek vůči eGC. Pravomoci Certifikačního orgánu, Odboru hlavního architekta eGovernmentu a RVIS při určení služeb, které mohou být provozovány v jednotlivých částech eGC (státní, komerční cloud), nejsou promítnuty nikde v předchozím textu, který se uvedeným vymezením zabývá (zejména kapitoly 5 a 6).

Kontakt pro vypořádání připomínek:
Mgr. Tereza Šamanová
225 279 603, tsamanova@spcr.cz