DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

Metodický návod pro orgány veřejné správy na využívání eGovernment cloudu ve veřejné správě

Obsah

1. Účel dokumentu

Tento dokument **popisuje pravidla a procesy využívání služeb eGovernment cloudu (dále jen „eGC“) ve veřejné správě** definované zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů (dále jen „ZoISVS“) a je vydán Digitální a informační Agenturou (dále jen „Agentura“), která je mimo jiné příslušným správním orgánem, který vede katalog cloud computingu (§ 6i odst. 2 ZoISVS) **Metodický návod je určen správcům informačních systémů veřejné správy (dále jen „ISVS“), kteří chtějí pro provoz svého ISVS využít služeb cloud computingu (dále jen „CC“).**

Orgán veřejné správy (dále jen „OVS“) metodický návod využívá při:

- podání žádosti o zápis poptávky cloud computingu[1],
- určení bezpečnostní úrovně poptávaného CC,
- definování možných variant provozu ISVS,
- hodnocení ekonomické výhodnosti jednotlivých variant provozu ISVS,
- stanovení bezpečnostních pravidel při využívání CC,
- přípravě zadávacího řízení na výběr poskytovatele CC,
- zápisu využívaného CC do katalogu CC[2].

2. Rozsah regulace cloud computingu podle ZoISVS

ZoISVS stanovuje práva a povinnosti, které souvisejí s vytvářením, správou, provozem, užíváním a rozvojem ISVS spravovaných státními orgány, orgány územních samosprávných celků nebo státními právnickými osobami (souhrnně jen „OVS“). ZoISVS ve své hlavě VI definuje i pravidla využívání služeb CC ve veřejné správě.

Některé OVS a ISVS jsou z působnosti zákona vyňaty:

- ZoISVS se nevztahuje na ISVS spravované (viz § 1, odst. 2):
  - pro potřeby nakládání s utajovanými informacemi,
  - zpravodajskými službami,
  - Národním bezpečnostním úřadem,
  - Národním úřadem pro kybernetickou a informační bezpečnost.
- ZoISVS se **s výjimkou vazeb na jiné informační systémy veřejné správy** nevztahuje na ISVS spravované (viz § 1, odst. 3):
  - pro potřeby zajišťování obrany státu,
  - pro potřeby podpory krizového řízení,

[1] Tato povinnost bude navržena ze ZoISVS vypustit, neboť se pro státní správu jedná o zbytečnou administrativní zátěž a v praxi se nevyužívá.

[2] Tato povinnost bude navržena ze ZoISVS vypustit, neboť se pro státní správu jedná o zbytečnou administrativní zátěž a v praxi se nevyužívá.

- orgány činnými v trestním řízení pro potřeby trestního řízení; zákon se vztahuje na evidenci Rejstříku trestů,
- bezpečnostními sbory,
- ozbrojenými silami České republiky nebo Vojenskou policií,
- Českou národní bankou,
- Finančním analytickým úřadem pro potřeby boje proti legalizaci výnosů z trestné činnosti nebo provádění mezinárodních sankcí za účelem udržování mezinárodního míru a bezpečnosti, ochrany základních lidských práv a boje proti terorismu,
- Ministerstvem vnitra pro potřeby provádění bezpečnostního řízení a vedení evidencí podle zákona upravujícího ochranu utajovaných informací a bezpečnostní způsobilost,
- Ministerstvem vnitra, Ministerstvem financí nebo Ministerstvem spravedlnosti pro potřeby zpracování osobních údajů příslušníků bezpečnostních sborů.

➢ ZoISVS se nevztahuje na provozní informační systémy (tj. systémy zajišťující pouze informační činnosti pro vnitřní provoz příslušného orgánu) **s výjimkou státními orgány spravovaných** (viz § 1, odst. 4):

- informačních systémů pro řízení a rozvoj lidských zdrojů a odměňování,
- elektronických systémů spisové služby (dále též "eSSL")[3],
- informačních systémů pro vedení účetnictví nebo řízení finančních zdrojů,
- systémů elektronické pošty.

➢ ZoISVS se nevztahuje na vazby provozních informačních systémů; to neplatí, jedná-li se o vazby provozních informačních systémů na jiné informační systémy veřejné správy, které nejsou provozními informačními systémy (viz § 1, odst. 5).

- týká se části provozního IS, která slouží k výměně dat s ISVS (pokud toto ISVS spadá pod rozsah regulace ZoISVS)

➢ Základní pravidla využívání cloud computingu orgánem veřejné správy, která definuje ZoISVS, se nevztahují na informační systémy, které slouží výlučně (§ 6l, odst. 4)[4]:

- ke správě a řešení technických potíží nebo diagnostice programových anebo technických prostředků, případně k zabezpečení nebo přenosu s tím souvisejících signálů,
- ke správě nebo využívání prostředků pro elektronickou identifikaci využívajících více faktorové autentizace,
- k aktualizaci nebo opravě programového prostředku, nebo
- ke shromažďování nebo výměně provozních údajů,

[3] Systém eSSL nebo účetnictví se považují za ISVS, jestliže zajišťují procesy nebo dílčí procesy agend úřadu.

[4] Podrobnější příklady scénářů pro body a) až d) jsou dále popsány v Příloze tohoto dokumentu.

- ke zkušebnímu provozu informačního systému veřejné správy, pokud při něm nebudou využity údaje, které se v informačním systému veřejné správy vedou nebo povedou anebo které jsou, nebo budou v souvislosti s poskytováním služby informačního systému veřejné správy využívány.[5]

I správci informačních systémů, na jejichž ISVS se ZoISVS nevztahuje, mohou služby zapsané v katalogu CC využívat. Výhodou v tomto případě je, že v katalogu CC jsou zapsáni prověření poskytovatelé a služby CC, tzn. služby vyhovují základním bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti služeb a zpracovávaných informací a u poskytovatele byl zkontrolován celý dodavatelský řetězec.

Pokud chce OVS využívat služby CC zapsané v katalogu i pro ISVS, na které se ZoISVS nevztahuje, a současně má OVS povinnost vést Informační koncepci, je v tomto případě nutné v ní zdůvodnit rozhodnutí využití nebo nevyužití cloudových služeb pro zajištění provozu svých ISVS (např. nedostatek zdrojů na ověření bezpečnosti poskytovatelů a jejich nabídek, nedostatek kapacit na zajištění dostatečné a požadované bezpečnosti).

[5] Viz www.dia.gov.cz/media/2479/download/Vyklad-ustanoveni-%C2%A7-6l-ZoISVS_231223.pdf

3. Používané pojmy[6]

Informačním systémem veřejné správy (ISVS) je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy nebo plnění jiných funkcí státu anebo dalších veřejnoprávních korporací. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále technické a programové prostředky, případně jiné nástroje umožňující výkon informačních činností. (viz ZoISVS § 2, odst. 1 písm. b)).

Provozním informačním systémem je informační systém veřejné správy zajišťující informační činnosti nutné pro vnitřní provoz příslušného orgánu (viz ZoISVS § 2, odst. 1 písm. q)).

Cloud computing (CC) je způsob zajištění provozu ISVS nebo jeho části prostřednictvím dálkového přístupu ke sdílenému technickému nebo programovému prostředku, který je zpřístupněný poskytovatelem cloud computingu a nastavitelný správcem ISVS (viz ZoISVS § 2, odst. 2).

Cloud computing zahrnuje služby třídy IaaS (Infrastructure as a Service), PaaS (Platform as a Service) a SaaS (Software as a Service) (viz standard Národního institutu standardů a technologií[7]). Pojem cloud computing nezahrnuje s cloud computingem úzce související profesionální služby podporující zavádění a správu CC (např. konzultační a integrační služby) ani dodávky nebo leasing hardware a software, ani služby housingu, ani služby telekomunikační infrastruktury ani služby uživatelské podpory.. Detailní vysvětlení, které služby patří do služeb CC a které ne, je uvedeno na webu Agentury[8].

Katalog cloud computingu je seznam, ve kterém se vedou údaje o poptávkách cloud computingu, poskytovatelích cloud computingu, nabídkách cloud computingu a o cloud computingu využívaném orgány veřejné správy (ZoISVS, § 6k, odst. 1).

Popis služeb CC v katalogu CC respektuje jednotnou hierarchickou strukturu služeb a jednotné parametry těchto služeb (Vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu, § 3 a § 4):

- třída služeb – IaaS (infrastruktura jako služba), PaaS (platforma jako služba) nebo SaaS (softwarová aplikace jako služba),
- oblast služeb – skupina obdobných typů služeb v rámci dané třídy služeb, které plní obdobnou základní funkcionalitu a jsou používány za stejným nebo podobným účelem (např. „databáze jako služba“ v třídě PaaS),
- typ služby – skupina obdobných konkrétních služeb, které mají stejný účel, obdobnou základní funkcionalitu a stejné základní parametry (např. „relační databáze“, specifický typ databáze v rámci oblasti služeb „databáze jako služba“),
- konkrétní služba – služba z nabídky, resp. ceníku poskytovatele.

[6] Tato kapitola uvádí definice, které jsou jednak definicemi zákona (v tomto případě je uveden odkaz na příslušnou legislativní normu) a jednak definicemi, které přidává tento návod.

[7] Viz National Institute of Standards and Technology

[8] Viz bod 1 https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/metodiky-navody-formulare/otazky-a-odpovedi-1

Poptávka cloud computingu je seznam typů služeb CC, které veřejná správa hodlá v daném období využívat pro provoz svých ISVS. Poptávku specifikuje Agentura souhrnně za celou veřejnou správu, a to jednak na základě vlastní analýzy a jednak na základě návrhů jednotlivých OVS[9].

Bezpečnostní úroveň pro využívání cloud computingu orgány veřejné správy[10] vyjadřuje možné dopady kybernetického bezpečnostního incidentu na poptávaný cloud computing. Bezpečnostní úrovně jsou nízká, střední, vysoká nebo kritická (Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, § 3) a určují se dopadovou analýzou dle kritérií daných vyhláškou.

Poskytovatel cloud computingu je subjekt, který poskytuje CC (přímo nebo nepřímo) orgánům veřejné správy. V souladu se ZoISVS musí být v katalogu CC zapsány všechny subjekty v rámci dodavatelského řetězce, tj.

- materiální poskytovatel CC, který službu CC produkuje na vlastní IT infrastruktuře, nebo na cloudové IT infrastruktuře jiného poskytovatele CC,
- distributor, který službu CC přeprodává jinému poskytovateli CC,
- koncový poskytovatel CC, který službu přímo nabízí OVS (může být i materiální poskytovatel).

Poskytovatel státního cloud computingu je osoba nebo jiné právní uspořádání, které je zřízené nebo založené státem, splňuje požadavky podle § 6m odst. 1 ZoISVS a je pověřené poskytováním cloud computingu orgánům veřejné správy. Jen poskytovatel státního cloud computingu je oprávněn poskytovat služby CC nejvyšší bezpečnostní úrovně, označované jako *kritická* (ZoISVS, § 6m, odst 2).

Nabídka cloud computingu je seznam konkrétních služeb CC jednotlivých zapsaných poskytovatelů CC, které úspěšně prošly ověřením (tzv. ex-ante kontrolou), že splňují požadavky dle zákona (ZoISVS § 6n a § 6t) a vyhlášky č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu, a to pro danou bezpečnostní úroveň.

Typ služby CC označuje množinu konkrétních služeb CC, které mají stejný účel a stejné druhy parametrů, které službu charakterizují. *Např. typ služby „Server bez operačního systému a bez hypervizoru" označuje celou řadu konkrétních virtuálních serverů. Tyto servery se dají charakterizovat těmito parametry: Typ vCPU, Frekvence, RAM, Server storage, Síťové připojení, Instance Sdílená/Dedikovaná/Rezervovaná, s/bez správy poskytovatelem.*

Konkrétní služba CC je služba CC, kterou nabízí poskytovatel CC ve svém ceníku. Konkrétní služba má vždy uvedeny hodnoty všech parametrů včetně místa zpracování dat nebo ceny.

[9] Pokud OVS plánuje poptávat typ služby, který nenalezne ve zveřejněné společné poptávce, nahlásí to Agentuře. Agentura návrh zváží a při nejbližší aktualizaci zahrne do nové verze společné poptávky cloud computingu.

[10] Výkladové stanovisko NÚKIB sjednocuje všechny povinnosti v oblasti regulace CC na OVS, viz https://nukib.gov.cz/download/publikace/podpurne_materialy/2023-07-14_vyklad-ust-par-4-odst-5_v1.1.pdf

4. Základní pravidla využívání katalogu CC

OVS může dle odst. 1 § 6l ZoISVS využívat pouze CC, který splňuje požadavky podle § 6n ZoISVS a je poskytovaný:

- poskytovatelem zapsaným v katalogu CC nebo poskytovatelem státního cloud computingu nebo
- v rámci obecné výjimky z povinnosti zadat veřejnou zakázku v zadávacím řízení podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen "ZZVZ")nebo
- v rámci vertikální nebo horizontální spolupráce podle ZZVZ.

V souladu s § 6n ZoISVS je nutné, aby byl v katalogu CC **zapsán jak poskytovatel** využívané služby, **tak konkrétní využívaná služba**.

Ustanovení § 6l ZoISVS odst. 4 uvádí **tzv. účelovou výjimku**, která stanoví patero účelů, pro něž lze využívat službu cloud computingu i bez splnění těchto podmínek[11].

Agentura pravidelně vytváří a publikuje na svém webu **společnou poptávku veřejné správy**[12]. Poskytovatel CC, který je již zapsán v Katalogu CC, zapisuje své konkrétní služby CC (pod názvy, které jsou v jeho ceníku) do Katalogu CC v jím zvolené bezpečnostní úrovni. Nabídka poskytovatele CC pak může zahrnovat i jiné služby, než jsou uvedeny v poptávce – tyto služby zařazeny pod typ „Ostatní".

Poskytovatel CC ve své nabídce zapisuje **služby v těchto skupinách**:

- služby třídy IaaS/PaaS/SaaS, které sám produkuje a nabízí,
- služby podpůrného CC, které pro své vlastní služby CC využívá,
- produkty a služby dodavatelů jiných služeb, než jsou služby cloud computingu, které daný poskytovatel využívá k realizaci svých služeb CC a u kterých může dojít ke zpracovávání informací orgánu veřejné správy, např. služby service desku,
- služby přeprodávaného CC, které produkuje jiný, „materiální", poskytovatel.

Je-li nabízená služba CC dodávána **řetězcem poskytovatelů CC**, pak každý poskytovatel tohoto řetězce musí být zapsán v katalogu CC. V katalogu CC musejí být zapsané i všechny služby CC dodavatelského řetězce, které jsou pro tvorbu služby nabízené zákazníkovi veřejné správy využívány (ZoISVS, § 6t).

[11] Viz www.dia.gov.cz/media/2479/download/Vyklad-ustanoveni-%C2%A7-6l-ZoISVS_231223.pdf

[12] Povinnost zapsat individuální poptávku bude navržena ze ZoISVS vypustit, neboť se pro státní správu jedná o zbytečnou administrativní zátěž a v praxi se nevyužívá. Tento krok není pro OVS před vyhlášením veřejné zakázky povinný.

5. Příprava na využití služeb CC

Následující kapitoly popisují doporučený postup, který lze použít při poptávání a využívání služeb cloud computingu ve veřejné správě. Některé kroky jsou obligatorní (vyplývají ze zákonů a vyhlášek), ostatní mají doporučující charakter.

Upozornění: **OVS v roli zadavatele musí vždy dodržovat ZZVZ.** Povinnostmi, které z tohoto zákona vyplývají, se tento dokument nezabývá.

Při přípravě vytvoření a rozvoje ISVS musí správce dle ZoISVS a dle vyhlášky č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy realizovat sám, resp. ve spolupráci s externím dodavatelem mj. tyto aktivity (bez ohledu na to, zda bude využívat CC nebo nikoliv):

a) dekomponovat ISVS na jednotlivé komponenty (není povinné),

b) zařadit ISVS (nebo jeho komponentu) do bezpečnostní úrovně,

c) zvážit modely cloud computingu, které by přicházely v úvahu pro realizaci a provoz ISVS (nebo jeho komponent), přičemž první volbou by mělo být využití modelu SaaS, pokud je k požadovanému typu v katalogu CC zapsána nějaká nabídka, teprve následně využití IaaS/PaaS[13],

d) vyhodnotit celkové náklady vlastnictví ISVS provozovaného různými modely,

e) ověřit, že v návrhu smlouvy jsou zahrnuta povinná bezpečnostní pravidla a adekvátní podmínky zpracování osobních údajů,

f) zavést/aktualizovat interní bezpečnostní politiku.

5.1 Dekompozice ISVS na jednotlivé komponenty (doporučeno)

Zajištění bezpečnosti ISVS je tím finančně náročnější, čím větší požadavky na bezpečnost ISVS správce klade. Proto je vhodné před využitím služeb CC dekomponovat ISVS na komponenty, jejichž nároky na bezpečnost se mohou lišit. Tato aktivita je sice fakultativní, ale je-li provedena dobře, může správci ISVS přinést značné finanční úspory.

Metodika dekompozice ISVS je uvedena na webu Agentury, bod 3 (Podpůrné materiály | DIA).

5.2 Zařazení do bezpečnostní úrovně

Obligatorní aktivitou správce ISVS (a to ať je ISVS provozován in-house, klasickým outsourcingem nebo pomocí služeb CC) je stanovení bezpečnostní úrovně ISVS (nízká, střední, vysoká, kritická). Jestliže byl ISVS dekomponován na jednotlivé komponenty, pak se stanovení bezpečnostní úrovně vztahuje jak na celý ISVS, tak na jeho jednotlivé komponenty – viz Vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy. Bezpečnostní opatření, která musí správce ISVS pro provoz komponenty zajistit, vyplývají na jedné straně z vyhl. č. 190/2023 Sb. (pokud je pro provoz komponenty využíván CC), a na druhé straně z vyhlášek o bezpečnostních opatřeních v režimu vyšších nebo nižších

[13] Jestliže se v katalogu CC taková nabídka/služba CC nevyskytuje, mělo by OVS informovat DIA, která tuto službu zahrne do společné poptávky, čímž dá signál poskytovatelům CC, aby takovou nabídku CC zapsali.

povinností dle nového ZKB č. 264/2025 Sb. (dále jen „nZKB"). Zde je třeba vzít v úvahu nový § 5b ZoISVS (vstupující v účinnost 1. 11. 2025), který přináší přiměřené plnění bezpečnostních opatření v režimu nižších povinností i pro OVS, které nejsou poskytovateli regulované služby dle nZKB, a to bez ohledu na využívání cloud computingu.

Metodika stanovení bezpečnostní úrovně ISVS je popsána na webu NÚKIB.[14]

5.3 Hodnocení TCO

Správce OVS musí provést hodnocení celkových nákladů vlastnictví ISVS (tzv. Total cost of ownership dále jen "TCO"), viz Vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy. V hodnocení se provádí srovnání různých variant realizace (např. ve variantě SaaS versus single-tenantní aplikace běžící na platformě IaaS/PaaS vs aplikace na míru provozovaná on-premise) a různými způsoby zajištění provozu aplikace (on-premise, cloud s administrací vlastními silami, cloud s externí administrací a podporou) při zohlednění požadavků, které jsou kladeny na určenou bezpečnostní úroveň. Pro vyhodnocení TCO různých variant realizace lze využít metodiku TCO a související kalkulátory[15].

5.4 Bezpečnostní opatření

Pro OVS vyplývají při využívání CC povinnosti z Vyhlášky č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
Tato vyhláška stanoví obsah a rozsah bezpečnostních pravidel, které buď musí OVS zahrnout do smluvního ujednání s poskytovatelem CC, nebo zavést interními opatřeními.

V příloze vyhlášky je uveden přehled vyžadovaných bezpečnostních opatření, která lze splnit několika různými způsoby, orientačně:

- řádky č. 1.1, 1.8, 1.14, 2.2, 5.1, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6,11.1, 12.1 lze nejlépe splnit **smluvními podmínkami s poskytovatelem cloudové služby** (a proto zde tyto požadavky uvádíme)

- řádky č. 1.2, 3.1, 5.2, 5.7, 6.1, 6.2, 9.2, 13.1, 15.2, jsou určeny ke splnění interními opatřeními na straně OVS;

- všechny ostatní řádky přílohy lze splnit vyjádřením poskytovatele CC (ke každému řádku zvlášť), jakým způsobem tyto řádky naplňuje (případně v kombinaci s bezpečnostními opatřeními na straně OVS), a to jednak na základě splnění požadavků zápisu nabídky dle vyhl. č. 316/2021 Sb., a dále na základě certifikací ISO 27001 / 27017 / 27018, resp. na základě auditních zpráv SOC 2 Type 2.

Agentura chystá k této povinnosti společně s NÚKIB podrobnější vodítko, které bude publikováno až po finalizaci a vydání nových verzí předmětných vyhlášek, které jsou nyní

[14] Národní úřad pro kybernetickou a informační bezpečnost – Materiály k regulaci cloud computingu a formulář, který lze využít je ke stažení zde https://nukib.gov.cz/images/Vzor_NUKIB-bezpecnostni-uroven-cloud_v1.0.xlsx .

[15] https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/metodiky-navody-formulare/metodika-tco-metodika-pro-vypocet-celkovych-nakladu-vlastnictvi-isvs

(září 2025) v připomínkovacím řízení.

Výběr modelu CC, který bude využit pro realizaci komponent ISVS

Pro výběr modelu CC, který bude využit pro realizaci komponent ISVS, přichází v úvahu celá řada variant, které vznikají vzájemnou kombinací následujících možností:

1) Kdo je dodavatelem softwarové aplikace?

- Poskytovatel SaaS

  V tomto případě poskytovatel dodává multi-tenantní aplikaci a zajišťuje její provoz na svojí nebo jím pronajaté platformě PaaS/IaaS. Současně zajišťuje i podporu provozu této aplikace, tzn. že integruje všechny služby, které jsou pro využívání aplikace potřebné.

- Poskytovatel single-tenantní aplikace provozované na cloudové infrastruktuře (IaaS/PaaS), který nabízí provoz aplikace jako službu

  V tomto případě poskytovatel provozuje pro objednatele dedikovanou instanci aplikace na vlastní cloudové infrastruktuře nebo na cloudové infrastruktuře třetí strany. Současně zajišťuje i podporu provozu této aplikace, tzn. že integruje všechny služby, které jsou pro využívání aplikace potřebné.

- Dodavatel softwarové aplikace (ať již standardní, nebo vyvinuté na míru)

  V tomto případě dodavatel nabízí licenci aplikace (nikoli formou služby) a případně její implementaci a zajištění provozu, ale aplikace je pak provozována na cloudové platformě PaaS/IaaS zajišťované objednatelem.

2) Kdo poskytuje platformní služby, na kterých je aplikace provozována?

- Dodavatel softwarové aplikace – viz 1 a) a b)
- Jiný poskytovatel než dodavatel softwarové aplikace – viz 1 c)

3) Kdo administruje platformní služby, na kterých je aplikace provozována?

- Poskytovatel aplikace
- Poskytovatel platformních služeb nebo jeho přeprodejce (na smluvní bázi)
- OVS vlastními zdroji
- Najatá specializovaná firma

Kombinací výše uvedených možností vzniká mnoho různých variant (modelů), které lze pro pořízení a provoz ISVS využít. V následujících subkapitolách jsou podrobněji popsány ty varianty, **které jsou v praxi nejčastější** (zejména pro malé a střední OVS).

A) Dodavatelem všech služeb souvisejících s vývojem, údržbou a provozem aplikace bude poskytovatel SaaS

Správce ISVS v této variantě vyhledá v katalogu CC, zda je v něm zapsána nabídka SaaS služby, která má správcem požadovanou funkcionalitu a bezpečnostní úroveň. Jestliže se

v katalogu CC taková nabídka nevyskytuje, mělo by OVS informovat DIA, která tuto službu zahrne do společné poptávky, čímž dá signál poskytovatelům CC, aby takovou nabídku CC zapsali.

S ohledem na žádoucí vyhnutí se možnému vendor-lock-in je vhodné, aby správcem požadovanou službu měli zapsanou v katalogu alespoň dva poskytovatelé, příp. aby alternativní aplikaci bylo možné pořídit v single-tenantním režimu na některé, v katalogu CC zapsané, platformě (IaaS/PaaS).

Dále správce IS pokračuje těmito kroky:

- Provede hodnocení celkových nákladů vlastnictví ISVS (TCO), a to se zvážením různých variant realizace (myšleno např. ve variantě SaaS versus single-tenantní aplikace běžící na platformě IaaS/PaaS) a různými způsoby zajištění provozu aplikace (on-premise, cloud s administrací vlastními silami, cloud s externí administrací a podporou). Pro vyhodnocení TCO různých variant realizace lze využít metodiku TCO a související kalkulátory.

- Toto hodnocení může být využito pro upřesnění předmětu veřejné zakázky (tzn. způsob využití cloudových služeb nebo on-premise řešení).

- Realizuje veřejnou zakázku na využití služeb CC6, s podmínkou, že služby, na které se vztahuje definice CC v ZoISVS, jsou zapsány v katalogu CC. Pro formulaci smlouvy s poskytovatelem SaaS správce může využít vzorovou smlouvu připravenou Agenturou[16].

B) OVS již vlastní licenci single-tenantní aplikaci, kterou provozuje on-premise, ale chce přejít s touto aplikací do cloudu a administrací cloudové platformy chce pověřit poskytovatele platformy

V tomto případě neexistuje k požadované aplikaci žádná zapsaná nabídka typu SaaS v katalogu CC.

Správce IS v tomto případě postupuje těmito kroky:

- Ve spolupráci se stávajícím dodavatelem aplikace identifikuje, které typy služeb IaaS/PaaS jsou potřebné pro provoz aplikace, a které již v katalogu CC zapsané platformy (kterých poskytovatelů) jsou podporovány pro provoz stávající aplikace,
- Vyčíslí, např. pomocí kalkulátoru TCO, celkové náklady vlastnictví aplikace při provozu on-premise, a z toho určí maximální výši infrastrukturních nákladů připadající na služby IaaS/PaaS, a to při zohlednění srovnatelných bezpečnostních opatření (v určené bezpečnostní úrovni),
- V katalogu CC vyhledá ty poskytovatele, kteří mají zapsané služby IaaS/PaaS v požadované nebo vyšší bezpečnostní úrovni, a současně vybere ty platformy IaaS/PaaS, které jsou podporované daným dodavatelem aplikace,
- Realizuje veřejnou zakázku na poskytovatele služeb IaaS/PaaS s těmito obligatorními podmínkami:

[16] https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/dynamicky-nakupni-system

- služby CC, které jsou součástí řešení, jsou zapsány v katalogu CC,
- poskytovatel bude zajišťovat i služby související s administrací platformy,
- zadavatel uvede v zadávací dokumentaci maximální výši infrastrukturních nákladů, kterou uchazeči v nabídkách nesmí překročit, jinak může zadavatel takové nabídky vyloučit.

C) OVS chce realizovat svoji agendu na míru šitou aplikací, jejíž vývoj zadá externímu dodavateli, ale současně požaduje, aby tato aplikace byla provozována v cloudu a administrovaná dodavatelem aplikace

Správce IS v tomto případě postupuje těmito kroky:

- Definuje požadovanou funkcionalitu a případně též požadovanou architekturu aplikace,
- Určí požadovanou bezpečnostní úroveň IS včetně případné dekompozice,
- Realizuje veřejnou zakázku na dodavatele aplikace a do obligatorních podmínek zahrne:

- dodavatel vyvine aplikaci s požadovanou funkcionalitou a architekturou,
- dodavatel vybere pro provoz aplikace vhodnou platformu s tím, že služby této platformy musí být vybrány ze zapsaných služeb IaaS/PaaS v katalogu CC s odpovídající bezpečnostní úrovní. Při výběru platformy lze přihlížet k již uzavřeným smlouvám OVS na dodávku cloudových služeb a k provozním zkušenostem ze strany OVS, případně k požadavkům informační koncepce úřadu,
- dodavatel současně zajistí administraci aplikace a administraci platformy, na které bude aplikace provozována.

6. Specifika veřejné zakázky při využívání služeb CC

Orgány veřejné správy mohou nakupovat služby cloud computingu buď individuálně (tj. přes samostatně organizované zadávací řízení) nebo přes centrálního zadavatele, kterým může být Agentura[17]. V obou případech je podmínkou využívání služby cloud computingu, že daný typ služby je zapsán v katalogu CC - [viz § 6l, bod 1, písm. a) ZoISVS].

Aktivity procesu veřejné zakázky definuje ZZVZ, proto je tato metodika nepopisuje. Soustředíme se pouze na aktivity, které jsou specifické při využití služeb CC pro provoz ISVS.

6.1 Minimální smluvní podmínky

Agentura připravila vzorovou smlouvu, která zahrnuje vyvážené smluvní podmínky, které by měly být akceptovatelné pro zadavatele i poskytovatele cloud computingu. Návrh vzorové smlouvy prošel předběžnou tržní konzultací.

Materiální poskytovatelé mají obvykle standardní návrh smlouvy, kterou může zadavatel také ve VZ akceptovat. Návrh vzorové smlouvy Agentury tuto skutečnost reflektuje, ale soustředí se i na problematiku implementace a akceptace služby do provozu.

Pokud z praktických důvodů nelze ve VZ využít návrh vzorové smlouvy, pak je nutné zajistit, aby smlouva s poskytovatelem CC zohlednila požadavky z vyhl. č. 190/2023 Sb. a Minimální smluvní podmínky[18].

6.2 Další doporučení týkající se veřejné zakázky a smlouvy

6.2.1 Vyzkoušet službu před uzavřením kontraktu

Zejména u služeb SaaS poskytovatelé obvykle nabízejí možnost vyzkoušení služby před tím, než zákazník smlouvu uzavře. Jestliže poskytovatel tuto možnost nabízí, je velmi vhodné tuto možnost využít. V testovacím režimu je vhodné zejména ověřit:

- vhodnost funkcionality,
- jednoduchost uživatelského rozhraní,
- dostupnost služby,
- dobu odezvy,
- možnosti administrace dané služby včetně změn objemu využívané služby,
- přehlednost reportingu o využívání služby,
- kvalitu podpory služby.

6.2.2 Aplikovat „multi-vendor strategy“

Pro snížení závislosti na jednom poskytovateli služeb CC a pro zjednodušení realizace případného přechodu k jinému poskytovateli služeb CC je vhodné aplikovat „multi-vendor strategy“. Ta je odlišná pro model SaaS a pro model IaaS/PaaS.

---

[17] https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/dynamicky-nakupni-system

[18] Viz bod 2 https://www.dia.gov.cz/cs/nase-cinnosti/na-cem-pracujeme/egovernment-cloud/metodiky-navody-formulare/podpurne-materialy

V návrhu smlouvy je vhodné požadovat po dodavateli pojistnou smlouvu v dostatečné výši, která odpovídá odhadované výši migračních nákladů (odhad z pohledu zadavatele), a to pro případ hrubého porušení smluvních podmínek.

Při využití modelu IaaS/PaaS je možné zvolit za dodavatele jednotlivých IaaS/PaaS služeb různé poskytovatele, přičemž je však třeba prověřit, jestli v případě jedné nebo více aplikací je možné nebo výhodné rozdělit provozní platformu IaaS/PaaS mezi několik různých poskytovatelů. Další hledisko je otázka odbornosti IT personálu: bude si více různých cloudových IaaS/PaaS platforem administrovat samo OVS, nebo bude administraci smluvně zajišťovat dodavatel aplikace? Podle těchto hledisek si OVS může v informační koncepci úřadu zdůvodnit omezení počtu různých cloudových platforem IaaS/PaaS, a další veřejné zakázky vypisovat s citací tohoto omezení podle přijaté informační koncepce úřadu.

6.2.3 Délka kontraktu

Protože trh s cloudovými službami se rychle vyvíjí (přibývají nové služby a mění se i jejich cenové relace) je vhodné pro délku kontraktu zvolit dobu neurčitou, kdy po předem zvolené minimální době kontraktu může zadavatel smlouvu vypovědět bez udání důvodu.

6.2.4 Škálování objemu odebíraných služeb

Služby CC jsou obvykle zpoplatňovány **modelem „pay-as-you-go“,** tj. zákazník platí pouze za ten objem služeb, který v uplynulém období (obvykle měsíc) spotřeboval. Smlouva obvykle také stanoví minimální a maximální objem spotřebované služby v daném období. Tato minimální a maximální hranice se může v průběhu smlouvy měnit. Zákazník by si proto měl zkalkulovat, jak se může měnit objem potřebných služeb v průběhu plnění smlouvy a ve smlouvě dohodnout v jakém předstihu a v jakých procentech může objem odebírané služby měnit.

Model „pay-as-you-go“ tedy umožňuje flexibilně škálovat skutečně čerpaný objem služeb a platit pouze za odebrané objemy, a také zjednodušuje případné předčasné ukončení smlouvy na žádost OVS.

V odůvodněných případech OVS může využít **alternativní model placení za služby CC**, který spočívá ve využití možných výrazných slev při zakázce na předplacené (rezervované) objemy služeb na budoucí období (typicky na 12 měsíců). Pokud OVS jedná v dobré víře, že danou službu bude ještě minimálně další rok muset zajišťovat s určitým průběhem čerpání, a má dobrou zkušenost nebo dobré reference na dodržování SLA poskytovaných služeb, může využít cenově výhodnějších nabídek na tyto „předplacené služby“. Je však třeba vzít v úvahu, že u těchto nákupů by v případě předčasného jednostranného ukončení smlouvy ze strany OVS tyto předplacené objemy čerpání mohly „propadnout“ bez náhrady. Pro předplacené služby na období 12 měsíců však může jít o akceptovatelné riziko podložené cenovou výhodností. Další výhodou zde může být smluvní závazek, že v případě celkového nárůstu poptávky služeb u daného poskytovatele může mít dané OVS prioritu při zajištění vyšší výpočetní kapacity v určitých kritických obdobích.

Typy služeb IaaS/PaaS je vhodné ve veřejné zakázce specifikovat formou spotřebního mixu (koše) typů služeb, který odpovídá kvalifikovanému odhadu např. roční spotřeby, a to s ohledem na časové rozložení (někdy lze již předem předpokládat zátěžovou špičku před určitým datem v roce).

6.3 Ceny služeb CC a celkové náklady provozu ISVS

Mezi hlavní cíle využívání CC ve veřejné správě patří snižování nákladů na vývoj a provoz ISVS při zajištění adekvátního zabezpečení ISVS a příp. dalších kvalitativních požadavků.

Vybere-li si OVS pro provoz svého ISVS některé ze zapsaných služeb CC, pak má jistotu, že tyto služby jsou dostatečně bezpečné pro provoz spravovaného ISVS.

K vyčíslení nákladů na vývoj a provoz ISVS napomáhá metodika kalkulace celkových nákladů ISVS. Metodika je doplněna nástrojem, který umožňuje spočítat celkové náklady vlastnictví (vývoje a provozu) ISVS za 5 let, a to jak s využitím on-premise provozu, tak s využitím služeb CC. Nejobvyklejší využití metodiky je v situaci, když se uvažuje o přechodu na provoz ISVS pomocí služeb CC a náklady této varianty provozu se porovnávají s náklady provozu ISVS v režimu on-premise, avšak za předpokladu zajištění srovnatelných bezpečnostních opatření.

Při kalkulaci nákladů na CC vzniká otázka, jak zjistit ceny jednotlivých služeb CC, které budou pro provoz ISVS využity. Existují tři varianty:

1) v kalkulaci se použijí ceny služeb CC, které jsou publikovány v zapsaných nabídkách CC v katalogu CC. Nevýhodou této varianty je, že v katalogu jsou uvedeny ceny z ceníku poskytovatele služby. Tato cena obvykle neobsahuje množstevní a další slevy, které může zákazník získat v konkrétní zakázce, a takto stanovená cena bývá u některých služeb vázána na jednotku využití (objem uložených nebo přenesených dat, počet provedených transakcí, využitý čas serverless operací, počet API volání), které lze bez pilotního provozu obtížně odhadnout,

2) v kalkulaci se použijí ceny, které uvedou jednotliví oslovení poskytovatelé v rámci RFI (Request for Information). Tato varianta dává obvykle přesnější výsledky než varianta první,

3) v kalkulaci se použijí ceny, které uvedou oslovení poskytovatelé ve svých nabídkách v rámci zadávacího řízení. Tato varianta dává nejpřesnější výsledky.

7. Význam zkratek

BÚ	bezpečnostní úroveň
CC	cloud computing
Agentura	Digitální a informační agentura
eGC	eGovernment Cloud
IaaS	infrastruktura jako služba
ISVS	informační systém veřejné správy
NIST	National Institute of Standards and Technology
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OVS	orgán veřejné správy
PaaS	platforma jako služba
SaaS	software jako služba
VS	veřejná správa
ZoKB	zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, v platném znění
ZoISVS	zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, v platném znění
ZZVZ	zákon č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

8. Související legislativa

8.1 Právní předpisy České republiky

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů – základní povinnosti v oblasti CC,

- Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu – konkrétní požadavky a postupy pro zápis cloudových služeb do katalogu CC,

- Vyhláška č. 433/2020 Sb., o údajích vedených v katalogu cloud computingu konkrétně stanovuje – jaké údaje musí být v katalogu CC vedeny a jakým způsobem mají být evidovány,

- Vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy – konkrétní pravidla a požadavky v oblasti CC pro OVS,

- Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci – určuje, ve které bezpečnostní úrovni má OVS poptávat služby CC,

- Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu – povinnosti a bezpečnostní pravidla pro OVS při využívání CC,

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti – stanovuje povinnosti v oblasti kybernetické bezpečnosti i pro cloudové služby,

- Zákon č. 134/2016 Sb., o zadávání veřejných zakázek – reguluje výběr poskytovatelů cloud služeb ve veřejné správě.

8.2 Právní předpisy Evropské unie

- Nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném pohybu těchto údajů (GDPR) - *reguluje zpracování osobních dat i v cloudových službách,*

- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2); byla implementována novým zákonem o kybernetické bezpečnosti č. 264/2025 Sb. - *zvyšuje požadavky na kybernetickou bezpečnost v klíčových sektorech*;

- Evropské schéma pro certifikaci cloudových služeb (EUCS - European Cybersecurity Certification Scheme for Cloud Services) je v procesu finalizace v rámci EU a bude pravděpodobně požadováno pro dodavatele poskytující služby veřejnému sektoru.

9. Příloha

9.1 Příklady „technických“ služeb cloud computingu mimo regulaci ZoISVS (dle § 6l odst. 4 písm. a) až d))[19]

a) Správa/řešení technických potíží, diagnostika, zabezpečení/přenos souvisejících signálů

Vzdálená podpora dodavatele účetního systému: technik dodavatele se jednorázově připojí (se souhlasem zákazníka) přes zabezpečený kanál a využije cloudovou službu, která si stáhne provozní logy, provede diagnostiku problému a odpojí se. (V tomto případě se neuplatní ZoISVS, ale celá aktivita musí proběhnout v souladu s GDPR (logy mohou obsahovat osobní údaje, které by neměly opustit EHP) a ZoKB, tj. aktivita musí proběhnout v souladu s podmínkami zpracování údajů, které plynou z povinností, které musí objednatel dodržovat. Tato poznámka platí i pro další příklady níže.)

AntiDDoS / aplikační firewall / řízení hrozeb „před“ webem nebo před emailovým systémem obce v cloudu: cloudová služba filtruje a přeposílá síťový provoz (např. eliminuje útoky zahlcením provozu), aktualizuje databáze signatur malwaru, vyhodnocuje podezření na malware a další hrozby. Služba sama nehostuje obsah webu nebo obsah emailů.

Monitoring dostupnosti: cloudová služba trvale ověřuje dostupnost webových stránek nebo serveru elektronické pošty a posílá notifikace (avšak nepracuje se zákaznickým obsahem).

Cloudová služba VPN: zajišťuje přenos signálů, ale neukládá obsahové informace.

Na co si dát pozor: pokud je součástí zkoumané cloudové služby i zpracování zákaznického obsahu nad rámec podpory / diagnostiky / zabezpečení / přenosu souvisejících signálů, pak již není možné tuto výjimku uplatnit.

b) Správa/využívání prostředků pro e-identifikaci s vícefaktorovou autentizací (MFA)

Cloudová správa a přenosy dat pro účely vícefaktorového přihlašování uživatelů: např. heslo + mobilní aplikace, One-Time-Password (OTP), hardwarový klíč.

Na co si dát pozor: tato výjimka se vztahuje jen na cloudovou správu a přenosy signálů prostředků pro elektronickou identifikaci a autentizaci – ne na jiná zákaznická data.

c) Aktualizace nebo oprava programového prostředku

Distribuce bezpečnostních záplat: scénáře související s aktualizacemi PC a serverů úřadu s využitím cloudových služeb výrobce softwaru.

Servisní zásah dodavatele: poskytnutí opravené verze aplikace s využitím cloudové služby a přes cloudové úložiště dodavatele.

Mobile Device Management (MDM): cloudová služba vzdáleně nainstaluje update do mobilů či tabletů, aniž by zpracovávala zákaznický obsah.

Na co si dát pozor: pokud služba aktualizace zároveň analyzuje či konvertuje obsah databáze nebo dokumentů zákazníka, zasahuje již mimo rozsah této výjimky.

---

[19] Tyto příklady nelze interpretovat tak, že se na zpracovávaná data nevztahuje další legislativa, např. GDPR, AI act, ZoKB

d) Shromažďování nebo výměna provozních údajů

Telemetrie a logy: přenos metadat typu čas, IP, chybové kódy, využití CPU, verze softwaru, pseudonym uživatele, a jejich agregace a vyhodnocování, bez samotného obsahu dokumentů či spisů.

Centrální dohled a správa logů: konsolidace provozních logů a jejich třídění, prohledávání, vyhodnocování, z důvodu auditu a řízení bezpečnosti.

Inventarizace licencí a verzí: sběr údajů „jaký software/která verze" běží na koncových stanicích.

Na co si dát pozor: „Provozní" versus „obsahová" data. Jakmile se přenáší, ukládají a vyhodnocují celé dokumenty, e-maily, soubory médií atd., výjimka se již neuplatní.