Souhrnná analytická zpráva

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

Projekt Příprava vybudování eGovernment cloudu	
Fáze:	Fáze I. (přípravná)
Úkol:	Předložit Vládě ke schválení souhrnnou analytickou zprávu v souladu se Strategickým rámcem Národního cloud computingu – eGovernment cloud ČR
Odpovědný subjekt:	Pracovní skupina RVIS pro přípravu vybudování eGovernment cloudu

Obsah

1 Úvod

1.1 Účel a příprava dokumentu

Dne 28.11.2016 schválila Vláda ČR *Strategický rámec Národního cloud computingu – eGovernment cloud ČR*. Vláda současně schválila založení pracovní skupiny RVIS a zahájení realizace projektu *Příprava vybudování eGovernment cloudu*. Schválený strategický rámec je odpovědí na úkol C7.1 (Vytvořit a vládě předložit Národní strategii cloud computingu) *Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2015 až 2020*, schváleného Vládou ČR 25.5.2015 *a* další podněty strategických dokumentů a kontrolních nálezů.

Strategický rámec definuje základní cíle eGC a základní koncepty eGC (rozdělení na komerční a státní část eGC, typy eGC služeb). Strategický rámec dále uvádí základní pravidla umísťování IS do eGC a rámcový harmonogram realizace, rozdělený do tří fází – přípravné, realizační a standardizační.

Záměrem projektu *Příprava vybudování eGovernment cloudu* je analýza legislativních, technických, ekonomických, organizačních a bezpečnostních podmínek vybudování eGovernment cloudu. Výstupem přípravné fáze projektu je souhrnná analytická zpráva (SAZ, tento dokument) obsahující kromě analýzy i návrhy opatření a doporučení implementačních kroků a standardů pro využívání cloud computingu ve veřejné správě. Souhrnná analytická zpráva bude předložena Vládě ČR ke schválení před zahájením realizační fáze.

Dne 9.12.2016 byla formálně ustanovena *Pracovní skupina RVIS pro přípravu vybudování eGovernment cloudu,* složená ze zástupců MV, MF, NBÚ/NÚKIB, zástupců ústředních orgánů státní správy, zástupců zpravodajských služeb a zástupců odborné veřejnosti. Pro přípravnou fázi projektu ustanovila pracovní skupina pět pracovních týmů:

- Legislativní/právní (L),
- Bezpečnostní (B),
- Ekonomická (E),
- Provozní/obsahová (P),
- Organizační/procesní (O).

Dokument se zaměřuje na formulaci a vysvětlení základních principů a mechanismů eGC. Jde primárně o dokument analytický, příklady a ukázky služeb eGC, katalogů eGC apod. Uvedené v tomto dokumentu nemají normativní, ale ilustrativní charakter. Rozpracování, aplikace v praxi a další rozvíjení popsaných principů je úlohou ŘOeGC.

Projekt *Příprava vybudování eGovernment cloudu ČR* je koordinován s přípravou strategie „**Digitální Česko**“, zejména s jejím pilířem „**Informační koncepce České republiky**“. Z pohledu strategie Digitální Česko a Informační koncepce ČR projekt *Příprava vybudování eGovernment cloudu ČR:*

- Přímo naplňuje dílčí cíl 5.5 (Vytvoření eGovernment cloudu).
- Přímo přispívá k naplnění dílčích cílů
  - 3.5 (META-informační systém (Meta-IS)),
  - 5.4 (Realizace optimálního modelu centrálního řízení státních organizací a podniků, specializovaných na poskytování ICT služeb),
  - 5.8 (Podpora budování agendových systémů v samosprávné působnosti, spisové služby a oběhu dokumentů a provozních systémů (Mail, ERP, HR)).
- Nepřímo přispívá k naplnění dílčích cílů
  - 2.9 (Vydat metodiku pro zadávání veřejných zakázek v oblasti ICT, případně upravit Zákon o veřejných zakázkách),

- 3.6 (Aktualizace a realizace strategie v oblasti budování a využívání komunikační infrastruktury veřejné správy),
- 5.3 (Zavedení principů a postupů „Enterprise architektury“),
- 5.6 (Vydání a aktualizace národních funkčních a servisních standardů).

1.2 Cíle projektu *Příprava vybudování eGovernment Cloudu*

Základním cílem eGC je **zvýšení efektivity, rozsahu poskytovaných služeb, kvality a bezpečnosti a zároveň snížení nákladů** provozu informačních systémů a aplikací veřejné správy, a to **využíváním sdílených ICT služeb** na úrovni infrastruktury, výpočetních platforem a standardizovatelných aplikací. To přináší mj.:

- zjednodušení a zrychlení nákupu standardních (komoditních) ICT služeb,
- sdílení datových center, komunikační infrastruktury, HW, základního SW, obslužného personálu a IT specialistů,
- standardizaci provozních a podpůrných aplikací,
- částečné řešení nedostatku ICT odborníků ve veřejné správě.

Součástí vybudování eGC je i **konsolidace datových center a HW platforem**, čímž se rozumí postupný přesun provozu většiny informačních systémů a aplikací veřejné správy z datových center jednotlivých institucí do vybraných datových center státu (státní část eGC), resp. Do datových center ověřených komerčních subjektů (komerční část eGC). Konsolidovaná infrastruktura a HW/SW platformy budou poskytovány formou **IaaS a PaaS služeb eGC**. Vybudování těchto služeb zahrnuje mj.:

- definici minimálních standardů pro poskytování IaaS a PaaS služeb pro státní a komerční část eGC,
- sjednocení provozního prostředí informačních systémů a aplikací provozovaných ve státní části eGC na několik vybraných platforem,
- zajištění potřebné bezpečnosti, spolehlivosti, škálovatelnosti a jednotnosti provozu ICT služeb.

Součástí vybudování eGC je dále postupná definice **standardů pro vybrané softwarové aplikace** podporující stejnou agendu či podpůrný a administrativní proces. Standardizované aplikační služby budou poskytovány formou **SaaS služeb eGC**. Využití standardizovaných aplikací přispěje ke standardizaci pracovních postupů (byznys procesů) ve veřejné správě.

eGC umožní organizacím veřejné správy, aby se více soustředily na svoje klíčové procesy místo podpůrných procesů typu zajištění provozu informačních systémů a aplikací. Organizace však musí i nadále být schopny definovat svoje požadavky na ICT služby a integrovat je do svých klíčových procesů.

Cíle projektu *Příprava vybudování eGovernment cloudu* jsou detailně popsány v příloze č. 1 *Cíle a měřitelné parametry budování a provozu eGC*. **Měřitelné parametry** jsou definovány v následujících oblastech:

- zvýšení rozsahu sdílení ICT zdrojů a ICT služeb VS,
- zrychlení a zefektivnění nákupu standardních (komoditních) ICT služeb,
- snížení nákladů na služby veřejné správy přepočtené na jednu ICT službu a jednoho uživatele,
- garance potřebné bezpečnosti a spolehlivosti provozu informačních systémů VS,
- odstranění legislativních překážek realizace eGC.

Tento dokument rozpracovává opatření, navržená v dokumentu *Strategie rozvoje ICT služeb veřejné správy*, schváleném usnesením Vlády ČR dne 2.11.2015, v části „Od izolovaných výpočetních systémů ke sdíleným ICT službám“. Jedná se o tato opatření:

- O21 Optimalizovat provozované ICT služby s využitím Katalogu provozovaných ICT služeb veřejné správy.
- O22 Nákup nových ICT služeb směřovat na sdílené služby s využitím tzv. eGovernment cloudu a Katalogu sdílených certifikovaných ICT služeb.
- O23 Vybudovat síť státních center sdílených služeb a regionálních datových center propojených bezpečnou datovou komunikační infrastrukturou, která budou poskytovat sdílené ICT služby orgánům veřejné moci.
- O24 Legislativně zakotvit způsob financování sdílených ICT služeb od jejich implementace až po udržitelnost provozu a nezbytný rozvoj.

1.3 Rozsah analýzy

Souhrnná analytická zpráva (tento dokument) obsahuje výsledky Fáze I. Projektu *Příprava vybudování eGovernment cloudu.* Cílem Fáze I. bylo provedení veškerých legislativně-právních, ekonomických, bezpečnostních a provozních analýz na úrovni detailu potřebné pro zahájení realizačních fází projektu, a to zejména stanovení:

- pravidel umísťování informačních systémů a aplikací veřejné správy do státní a komerční části eGC, včetně detailní metodiky určování bezpečnostních a ekonomických kritérií,
- definice typů a struktury služeb eGC, včetně standardů popisu služeb eGC a smluvních podmínek,
- bezpečnostních a provozních standardů služeb eGC,
- právního rámce státní a komerční části eGC,
- definice řídících orgánů eGC a jejich rolí,
- procesního modelu státní a komerční části eGC z pohledu zákazníka (správce IS), provozovatele služeb eGC a řídících orgánů eGC,
- návrhu legislativních úprav a podzákonných norem, včetně nařízení Vlády pro období do schválení legislativních změn,
- časového plánu dalších fází projektu *Příprava vybudování eGovernment cloudu*.

Součástí výstupů Fáze I. není určení souhrnných kapacitních a finančních parametrů eGC jako celku ani konkrétních plánů migrace informačních systémů a aplikací do eGC. Důvodem je časová náročnost sběru podkladů z jednotlivých organizací veřejné správy. Dokument obsahuje metodiku a časový plán shromáždění podkladů (katalogů informačních systémů, aplikací a datových center, určení ekonomických a bezpečnostních kritérií pro umístění do eGC) pro následné vyhodnocení v další fázi projektu.

1.4 Struktura dokumentu

Základní struktura dokumentu vychází z kombinace pohledů ze strany poptávky (Správci IS – zákazníci eGC), ze strany nabídky (Provozovatelé eGC, právní rámec komerční a státní části eGC) a ze strany řízení služeb eGC (Řídící orgán eGC). Detailnímu zpracování problematiky příslušné jednotlivým pohledům jsou věnovány samostatné kapitoly.

Jednotlivé pohledy ze strany poptávky a nabídky, resp. Provozu a řízení se potkávají v řadě míst (např. Katalog služeb eGC, bezpečnostní úrovně, způsob nákupu a smluvní rámec služeb eGC). V těchto případech je vždy jeden z pohledů zvolen jako primární místo pro popis dané problematiky a ostatní pohledy se na něj odkazují.

Dokument uvádí dvě přehledové kapitoly, věnované popisu aktuálního stavu IS veřejné správy a celkovému konceptu eGC (definice hlavních pojmů eGC, základní pravidla a principy eGC a přehled základních procesů eGC).

Závěrečná kapitola obsahuje projektový pohled na další fáze budování eGC.

1.5 Přílohy

Přílohy obsahují detailnější rozpracování vybraných metodických postupů uvedených v tomto dokumentu. Obsah příloh bude dále rozpracován a udržován ŘOeGC.

Příloha č. 1 – Cíle a měřitelné parametry budování a provozu eGC

Příloha č. 2 – Katalog aktuálně provozovaných IS

Příloha č. 3 – Metodika kalkulace TCO

Příloha č. 4 – Metodika stanovení požadavků na bezpečnost IS

Příloha č. 5 – Minimální smluvní podmínky

2 Manažerské shrnutí

Souhrnná analytická zpráva projektu *Příprava vybudování eGovernment cloudu* (SAZ, tento dokument) zpracovává na základě schváleného *Strategického rámce Národního cloud computingu – eGovernment cloud ČR* analýzu legislativních, technických, ekonomických, organizačních a bezpečnostních podmínek vybudování eGovernment cloudu (eGC). Dokument vznikl v rámci činnosti P*racovní skupiny RVIS pro přípravu vybudování eGovernment cloudu,* složené ze zástupců MV, MF, NBÚ/NÚKIB, zástupců ústředních orgánů státní správy, zástupců zpravodajských služeb a zástupců odborné veřejnosti. Při tvorbě dokumentu byly zohledněny požadavky resortů a zkušenosti zemí EU, které již government cloud provozují (zejména Velké Británie, Dánska a Estonska).

Projekt *Příprava vybudování eGovernment cloudu ČR* je koordinován s přípravou strategie „Digitální Česko“, zejména s jejím pilířem „Informační koncepce České republiky“. Projekt přímo naplňuje dílčí cíl 5.5 Informační koncepce ČR (Vytvoření eGovernment cloudu) a dále přímo nebo nepřímo přispívá k naplnění řady dalších dílčích cílů.

Základním cílem eGC je zvýšení efektivity, kvality a bezpečnosti a zároveň snížení nákladů provozu informačních systémů a aplikací veřejné správy využíváním sdílených cloudových služeb eGC. Cílem projektu je zároveň v maximální míře usnadnit jednotlivým správcům IS architektonické, bezpečnostní, nákupní a projektové procesy využívání služeb eGC. Z celkového a dlouhodobého pohledu je souvisejícím cílem eGC i konsolidace datových center a HW platforem veřejné správy do datových center provozovatelů eGC. Dokumentem se proto prolínají dva pohledy na eGC – pohled definice služeb eGC a jejich využití v rámci jednoho IS a pohled řízení dlouhodobé postupné migrace významné části IS veřejné správy v ČR na služby eGC.

Dokument stručně shrnuje aktuální stav IS veřejné správy a jeho nedostatky, k jejichž řešení eGC přispívá. Cca 7500 OVM má dohromady registrováno cca 7500 různých IS, z čehož velká část (zejména u IS samospráv) jsou izolovaně nakupované a provozované, ale přitom navzájem prakticky stejné systémy. Většina IS je pořizována jako jednotný komplexní celek včetně HW a provozních služeb a není zpracováno mapování jejich struktury na standardizovanou čtyřvrstvou architekturu eGovernmentu ani standardizovaná struktura jejich investičních a provozních nákladů, což významně komplikuje řízení ICT nákladů veřejné správy. Průzkumy datových center státních institucí uvádějí vysoké počty malých datových center jednotlivých institucí, z nichž velká část (85% při průzkumu 47 datových center v roce 2015) je technologicky a provozně nevyhovující. Rychlost rozvoje IS je v mnoha případech významně omezena časovými prodlevami při přípravě a organizaci velkých a komplexních veřejných ICT zakázek. Služby státních ICT podniků jsou dostupné pouze resortům jejich zakladatelů.

Odhady celkových ročních nákladů veřejné správy na IT se pohybují podle úhlu pohledu a dostupných evidencí od 6,5 mld. Kč (provozní náklady IS registrovaných v ISoISVS) po 15,8 mld. Kč (investiční i provozní výdaje vybraných položek státního rozpočtu). Uvážíme-li cílový odhad globálních úspor z využití eGC - 20%, což je konzervativní odhad vycházející ze zahraničních zkušeností, pak by roční úspory při využití eGC mohly být v řádu miliard Kč. Důležitým ekonomickým aspektem využívání služeb eGC bude postupný přechod od investičního financování (částí) IS k provoznímu financování.

Služby eGC zahrnují tři hlavní kategorie cloudových služeb: IaaS (Infrastructure as a Service – služby na úrovni datových center, sítí a HW), PaaS (Platform as a Service – služby na úrovni standardních SW platforem, jako jsou databáze, webové servery) a SaaS (Software as a Service – kompletní funkcionalita standardních nebo standardizovatelných aplikací poskytovaná jako služba, např. e-mail, ekonomický systém, spisová služba apod.). Z dlouhodobého pohledu je využití služeb na úrovních IaaS a PaaS předpokládáno primárně jako sdílené platformy na nižších úrovních architektury specifických agendových systémů jednotlivých organizací veřejné správy a služby SaaS pro řešení standardních agendových

systémů samosprávy a standardních provozních systémů všech organizací veřejné správy. Služby eGC budou evidovány a popsány jednotným způsobem v Katalogu služeb eGC.

Dokument a jeho přílohy definují detailní metodiku hodnocení úrovně bezpečnostních dopadů IS, která rozděluje IS do bezpečnostních úrovní 1-4 (Nízká, Střední, Vysoká, Kritická). V odpovídajících úrovních pak definuje bezpečnostní požadavky na služby eGC. Dokument a jeho přílohy dále definují detailní metodiku kalkulace celkových nákladů vlastnictví (TCO) jednotlivých IS v modelu provozu on-premise (na vlastní infrastruktuře) a s využitím služeb eGC. Výsledky hodnocení IS podle obou metodik budou evidovány v rozšířených katalozích aplikací veřejné správy (ISoISVS, resp. RPP) a jsou důležitými parametry pro pravidla umísťování IS do eGC.

V následující fázi budování eGC, dlouhé zhruba dva roky, bude umísťování IS do eGC (využívání služeb eGC) dobrovolné. Dlouhodobě bude pro naprostou většinu OSS uplatněn princip cloud-first – povinné umístění jejich IS do eGC, pokud kalkulace TCO neprokáže nákladově efektivnější provoz on-premise. Umístění IS samosprávy do eGC zůstane dlouhodobě dobrovolné, nicméně lze předpokládat, že provoz do velké míry standardizovaných systémů samosprávy bude v prostředí sdílených služeb eGC efektivnější a levnější než on-premise řešení.

eGC je rozdělen do dvou částí - komerční část (KeGC - služby provozované komerčními subjekty s využitím jejich vlastních datových center a komunikační infrastruktury) a státní část (SeGC – služby provozované v datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem). Kritériem pro využití služeb SeGC nebo KeGC je úroveň bezpečnostních dopadů daného IS. SeGC zajistí maximální úroveň bezpečnosti a je určen pro provoz služeb eGC bezpečnostní úrovně 4 (Kritická). KeGC v maximální míře využije tržních mechanismů pro zajištění optimálních cen pro nižší bezpečnostní úrovně. Dokument stanovuje bezpečnostní a provozní požadavky závazné pro KeGC i SeGC.

Nákup služeb KeGC bude realizován prostřednictvím centrálně řízeného soutěžního mechanismu (dynamického nákupního systému), který zajistí nejen optimální ceny, ale i co nejvyšší míru standardizace nakupovaných služeb. Právní rámec SeGC bude zvolen na základě legislativního rozboru variant a doporučení meziresortní komise garantů jednotlivých relevantních zákonů – MV (ZoISVS), MF (ZoRP), MPO (ZoSP) a MMR (ZZVZ) – ve spolupráci s pracovní skupinou RVIS pro přípravu vybudování eGovernment cloudu a na základě požadavků, kritérií a variant uvedených v tomto dokumentu, do 30.6.2019. Pracovní skupina RVIS doporučuje variantu „nový státní podnik určený pro poskytování služeb SeGC, zřízený zákonem“, která umožní všem OSS nakupovat eGC služby na základě výjimky ze ZZVZ.

Na úrovni centrálního řízení eGC dokument definuje Řídící orgán eGC (ŘOeGC), který bude koordinovat budování a rozvoj eGC, rozvíjet a udržovat metodické postupy definované v tomto dokumentu, kontrolovat a řídit soutěžní mechanismus KeGC a nabídku služeb SeGC. ŘOeGC bude spravovat Portál eGC, na kterém bude zveřejňovat Katalogy služeb eGC a poskytovat správcům IS informační a metodickou podporu pro využívání eGC.

Dokument obsahuje plán dalších kroků budování eGC, zejména ustanovení ŘOeGC a SeGC a pilotní projekty KeGC, SeGC a Portálu eGC. Nejbližším analytickým krokem je sběr informací od potenciálních zákazníků eGC a detailní stanovení konkrétních celkových plánů ekonomických, kapacitních a plánu migrace. Dokument dále obsahuje přehled navrhovaných legislativních změn, které mají být v následující fázi rozpracovány a předloženy ke schválení.

3 Aktuální stav a jeho nedostatky

Tato kapitola uvádí stručný popis aktuálního stavu informačních systémů veřejné správy, pravidel jejich rozvoje a provozu, zaměřuje se na nedostatky aktuálního stavu, které pomůže vyřešit eGovernment cloud.

3.1 Stav informačních systémů veřejné správy

Dokument *Strategie rozvoje ICT služeb veřejné správy*, schválený usnesením Vlády ČR dne 2.11.2015, popisuje nedostatky současného stavu řízení a provozování ICT ve veřejné správě. Z nich vyjímáme ty, na jejichž odstranění je zaměřeno zavedení eGC:

- **N04** - ve veřejné správě je běžné, že aplikace se stejnou funkcionalitou (mzdy, účetnictví, spisová služba, e-mail, kancelářské aplikace atd.) a jejich technologická infrastruktura (servery, operační systémy, databázové systémy atd.) jsou jednotlivými OVM nakupovány a provozovány multiplicitně, izolovaně a nezávisle na sobě. To vede k plýtvání s finančními prostředky státu.
- **N06** - neexistují jednotná pravidla sledování nákladů (investičních a provozních) ICT služeb. Z toho plyne, že finanční údaje o investičních a provozních nákladech ISVS jsou nevěrohodné. To má mimo jiné za důsledek, že vláda, zákonodárci ani jednotlivé OVM nemají kvalitní informace o tom, jaké jsou celkové roční náklady ICT služeb (např. náklady na spisovou službu, na e-mail atd.), jaká je struktura těchto nákladů, ani o tom, jak se liší náklady různých poskytovatelů téže služby. To komplikuje manažerská rozhodnutí na úrovni vlády, ministerstev i jednotlivých OVM.

Rozsah prvního problému demonstrují následující čísla (dle údajů https://www.sluzby-isvs.cz/ ke dni 25.7.2017):

- počet OVM je cca 7500,
- počet registrovaných informačních systémů VS je celkem 7 408.

Vzhledem k tomu, že počet různých typů aplikací veřejné správy je maximálně několik set, tyto údaje jasně dokumentují multiplicitní výskyt aplikací se stejnou funkcionalitou.

Problematiku vytváření, správy, provozu, užívání a rozvoje informačních systémů veřejné správy (ISVS) upravuje **zákon č. 365/2000 Sb., o informačních systémech veřejné správy** (ZoISVS), jehož novelizace proběhla v roce 2017. ZoISVS reguluje primárně informační systémy podporující agendy veřejné správy. Z provozních informačních systémů zahrnuje pouze ty nejvýznamnější, v oblasti personalistiky, spisových služeb, ekonomických systémů a elektronické pošty. ZoISVS se dále zaměřuje primárně na ISVS provozované organizacemi státní správy a obcí, které vykonávají státní správu v přenesené působnosti.

Vyhláška č. 529/2006 Sb. o dlouhodobém řízení ISVS stanovuje požadavky na strukturu a obsah informační koncepce, kterou dle ZoISVS vytvářejí a aktualizují jednotlivé orgány veřejné správy.

Vyhláška č. 528/2006 Sb. o informačním systému o ISVS zavádí informační systém ISoISVS, který obsahuje základní informace o dostupnosti a obsahu ISVS.

3.2 Principy architektury eGovernmentu

Řada strategických dokumentů vytvořených Odborem hlavního architekta eGovernmentu Ministerstvem vnitra, zavádí principy a pravidla architektury eGovernmentu ČR, založené na principech enterprise architektury

- Strategický rámec rozvoje eGovernmentu 2014+, Ministerstvo vnitra 2014,

- *Strategie rozvoje ICT služeb veřejné správy*, schválená usnesením Vlády ČR dne 2.11.2015, popisuje nedostatky současného stavu řízení a provozování ICT ve veřejné správě a definuje základní cíle vytvoření a řízení Národní architektury eGovernmentu,
- Materiály OHA MV – Národní architektura veřejné správy (NA), Národní architektonický rámec (NAR), Národní architektonický plán (NAP), Architektonické vzory sdílených služeb.

Zatímco ZoISVS vnímá ISVS jako samostatné monolitické celky bez důrazu na jejich vnitřní strukturu, národní architektura veřejné správy zavádí model **čtyřvrstvé architektury eGovernmentu** a standardní strukturu architektonických domén pro popis architektury jednotlivých ISVS:

- architektura výkonu a provozu veřejné správy (Služby veřejné správy, Byznys vrstva),
- architektura informačních systémů (Služby informačních systémů, Aplikační vrstva),
- architektura IT HW/SW technologické infrastruktury (Služby platforem IT, Technologická vrstva),
- architektura komunikační technologické infrastruktury (Služby komunikační infrastruktury, Komunikační vrstva).

Národní architektonický plán dále definuje roli a způsob použití sdílených centrálních služeb eGovernmentu, jako např. Propojený datový fond (základní registry, eGSB), elektronické doručování (datové schránky), kontaktní místa (PVS, CzechPoint), správu identit (JIP/KAAS, NIA).

Usnesení vlády č. 889 ze dne 2. 11. 2015 a dále novela ZoISVS z roku 2018 zavádí povinnost pro organizační složky státu získat **stanovisko OHA k** projektům s předpokládanou hodnotou přesahující 6 miliónů Kč za rok. Žádost o stanovisko OHA obsahuje popis předmětného IS v kontextu čtyřvrstvé architektury eGovernmentu a popis využití sdílených služeb eGovernmentu. Usnesení vlády č. 889/2015, spolu s obdobným požadavkem vybraných výzev *Integrovaného regionálního operačního programu* (financování EU), se stalo klíčovým stimulem naplňování principů architektury eGovernmentu. *Zprávy o posuzování projektů Útvarem Hlavního architekta eGovernmentu* (Ministerstvo vnitra, 2016, 2017) uvádí statistiku 115 posouzených projektů v celkové hodnotě 19,1 miliardy Kč v roce 2016 a 357 posouzených žádostí o stanovisko k ICT projektům v celkové hodnotě 24,8 miliardy Kč za rok 2017.

Národní architektura veřejné správy se v současné verzi zabývá sdílením zdrojů a standardizovaných ICT služeb na úrovni technologické vrstvy pouze okrajově, nicméně je s konceptem eGC plně kompatibilní. Architektura eGovernmentu ČR se vyvíjí v čase a je postupně kodifikována v nových vládních, zákonných a podzákonných normách. V současné době je připravována nová verze *Informační koncepce České republiky* (podle ZoISVS) a návazných dokumentů, jejíž příprava je synchronizována s projektem *Příprava vybudování eGovernment cloudu*. Nová informační koncepce určí architektonická a procesní pravidla pro poskytovatele sdílených služeb, správce jednotlivých ISVS a celkovou enterprise architekturu (architekturu úřadu) jednotlivých OVM. eGC zapadá do architektury eGovernmentu ČR jako nový typ sdílených služeb – primárně na technologické vrstvě (IaaS, PaaS) a aplikační vrstvě (SaaS).

3.3 Aktuální stav datových center VS

Dalším nedostatkem, jehož odstranění eGC přináší, je nedostatečná bezpečnost a spolehlivost datových center jednotlivých institucí státu.

2015 - průzkum SPCSS stavu datových center státních institucí

V průběhu roku 2015 provedla Státní pokladna Centrum sdílených služeb, s.p. průzkum stavu datových center státních institucí. Předmětem hodnocení byl technologický management

datových center a serverových místností. Zpracovány byly dotazníky obsahující data o 47 datových centrech a serverových místnostech organizací státní správy. Dotazník obsahoval 152 otázek hodnotících jejich dílčí parametry, které byly rozděleny do následujících sekcí:

- kapacita a spolehlivost síťového připojení,
- konektivita k internetu,
- obecné vlastnosti datového centra,
- vstupní kontrola,
- lokalita,
- generátory a palivové nádrže,
- procesní zabezpečení.

Z celkového počtu hodnocených 47 datových center a serverových místností bylo hodnoceno:

- 0 % plně vyhovujících,
- 15 % dostatečných,
- 85 % nevyhovujících.

Ze 152 parametrů bylo 50 identifikováno jako kritické.

- Ani jeden kritický parametr nebyl splněn ve všech DC.
- Žádné DC nesplnilo všechny kritické parametry.
- Pouze 10 ze 46 hodnocených DC splnilo alespoň 80 % kritických parametrů.

Závěry z průzkumu: Základním rizikem, které doprovází uchovávání dat ve státní a veřejné správě je v prvé řadě absence koncepčního řešení rozvoje datových center a uchovávání státních dat jako celku. Jednotlivé subjekty státní a veřejné správy nemají dlouhodobě koncepčně vyřešen provoz, vybavení zabezpečení a rozvoj datových center jednotlivých resortů. Není tedy možné efektivně plánovat investice do datových center, HW a zabezpečení a citlivá data jednotlivých státních subjektů jsou de facto uchovávána v nevyhovujících prostorech a na zastaralé infrastruktuře. K dalším rizikům, která je možné v této oblasti identifikovat, patří především nemožnost a počáteční nereálnost odhadu budoucí potřebné kapacity datového centra. Následně pak dochází k poddimenzování kapacity, nebo naopak ke zbytečně vynaloženým nákladům z veřejných rozpočtů. Provoz vlastního datového centra rovněž vyžaduje odborné personální zajištění, a především zvládnutí fyzické a logické bezpečnosti uložených dat. Tyto nároky mnohdy subjekty státní správy nejsou schopny plnit vlastní silou a dochází tak ke značným rizikům, která mohou mít za následek ohrožení celého datového fondu.

2017 – dotazníkové šetření RVIS

V roce 2017 provedl RVIS stručné dotazníkové šetření stavu datových center OSS, zaměřené na identifikaci volných kapacit. Z pohledu hodnocení kvality datových center průzkum obsahoval otázky na vlastní orientační hodnocení podle stupnice Tier I-IV (Uptime Institute). Celkově bylo hodnoceno 88 odpovědí.

- Pouze pro dvě datová centra byla uvedena volná kapacita nebo možnost rozšíření v rozsahu vyšších desítek m2 (SPCSS, MPSV).
- Pouze 12 organizací hodnotí kvalitu svých datových center na úrovni Tier III a jedna na úrovni Tier IV.

3.4 Legislativa a veřejné zakázky

Rychlost rozvoje IS je v mnoha případech významně omezena časovými prodlevami při přípravě a organizaci veřejných zakázek v oblasti ICT mj. Z následujících důvodů

- Řada veřejných zadavatelů prochází složitým procesem zbavování se závislosti na stávajících dodavatelích.
- Klesá míra využívání JŘBU a narůstá počet vypisovaných otevřených výběrových řízení.
- Veřejné zakázky na velká komplexní ICT řešení probíhají v extrémně kompetitivním prostředí s častým použitím námitek proti zadávací dokumentaci a rozhodnutí zadavatele nebo s podáním k ÚOHS.

Výše uvedené faktory významně zvyšují požadavky na kvalitu přípravy veřejných zakázek.

Služby státních ICT podniků, které mohou zmírnit některé z uvedených faktorů, jsou dostupné pouze resortům jejich zakladatelů.

3.5 Ekonomický pohled na sdílené služby

Pro určení celkových nákladů na investice a provoz neexistuje jednotná a exaktní metodika, lze zvolit několik pohledů.

1) Z pohledu nákladů registrovaných v ISoISVS (pročištěné údaje únor 2018) jsou **celkové investiční náklady registrovaných ISVS 38,8 mld. Kč** (30,2 mld. státní správa, 8,2 mld. samospráva, 0,4 mld. ostatní) a **roční provozní náklady jsou 6,4 mld. Kč** (státní správa 4,9 mld., samospráva 1,4 mld., ostatní 0,1 mld.).
2) Z pohledů rozpočtových výdajů (monitor.státnipokladna.cz) při uvážení pouze rozpočtových položek 5042, 5168, 5172, 6111, 6125, 5137, na kterých jsou evidovány převážně ICT výdaje, **roční výdaje (investiční i provozní) mezi roky 2010 a 2016 postupně rostou od 9 mld. Kč do 15,8 mld. Kč.** To nezahrnuje výdaje evidované společně s non-IT výdaji v dalších položkách a zároveň zahrnuje i některé non-IT výdaje evidované v uvedených položkách. Poznámka: Pro tuto orientační kalkulaci byla zvolena nejbližší reprezentativní sada rozpočtových položek.
3) Z pohledu objemu zadávaných veřejných zakázek v oblasti ICT (Výroční zpráva MMR o stavu VZ v ČR) byly v **roce 2014 zadány veřejné zakázky za 19,2 mld. Kč**. To nezahrnuje zakázky zadané na základě výjimek ze ZVZ/ZZVZ.

Zkušenosti Velké Británie, Dánska a dalších zemí ukazují úspory při přechodu z nesdílených na sdílené služby formou eGC 10% až 50%. Uvážíme-li konzervativní cílový odhad 20% úspor, pak by roční úspory při využití eGC mohly být v řádu miliard Kč.

Například Správa základních registrů, jako jedna z podřízených organizačních složek státu MV nyní plánuje obnovu celého systému základních registrů, kde hrubým quick-scanem bylo zjištěno, že vybudování cloudového řešení pro všech šest systémů bude finančně 3-4x méně náročné pro rozpočet státu, než když by se měly budovat autonomní řešení *(Poznámka: jedná se o plnění usnesení vlády ČR ze dne 31. května 2017 č. 411 ke Zprávě o potřebě zahájení transformačního projektu řešícího obnovu a systémový rozvoj základních registrů návazných systémů, na základě něhož nyní probíhá projekt).*

Aktuální stav v rámci definice výhodnosti pořizování autonomního nebo sdíleného ICT prostředí a současně **výpočtu TCO** lze shrnout tak, že existuje jediné pravidlo/metodika pro výpočet výdajů, souvisejících s pořizováním, obnovou technologií. Jedná se o usnesení vlády ČR ze dne 2. listopadu 2015 č. 889/2015 k dalšímu rozvoji informačních a komunikačních technologií služeb veřejné správy a to: *Základní zásady postupu při čerpání finančních prostředků na výdaje související s informačními a komunikačními technologiemi s hodnotou více než 6 mil. Kč ročně, uvedené v příloze č. 2 tohoto usnesení (dále jen „Základní zásady“).*

Součástí Základních zásad je *Metodika výpočtu TCO ICT služeb veřejné správy*. Podle těchto pravidel jsou OHA MV předkládány požadavky na budování, opravy a rozvoj autonomních informačních systémů. Z ekonomického pohledu však tato pravidla neurčují a nijak nevymezují,

jak na základě příslušné legislativy může veřejná správa sdílet výpočetní výkon a popřípadě i systémy. Lze tedy konstatovat, že v ČR **neexistují pravidla ani praktický nástroj pro potřeby organizací veřejné správy k posouzení ekonomické výhodnosti pořízení a provozu požadované sdílené ICT služby**.

3.6 Bezpečnost informačních systémů veřejné správy

Bezpečnost ISVS je v současné době vymezena pouze zmínkou v článku o **dlouhodobém řízení ISVS** (§5a) zákona č. 365/2000 Sb., o informačních systémech veřejné správy, a **obecným požadavkem uplatňování bezpečnostních opatření pro** zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v ISVS (§5b). Vyhláška č. 529/2006 Sb. pak v §4 uvádí stanovení požadavků na bezpečnost ISVS jako povinnou součást informační koncepce, a požaduje zpracování plánu řízení bezpečnosti a popisu činností nutných pro dosažení stanovených požadavků na bezpečnost. Dále vyhláška stanoví v §10 požadavek zpracovat bezpečnostní politiku a bezpečnostní směrnice v rámci povinné bezpečnostní dokumentace ISVS. Tyto právní předpisy však nepracují s pojmy, jako je hodnocení dopadů ztráty důvěrnosti, integrity a dostupnosti zpracovávaných dat nebo celé služby na chod organizace příp. celou společnost, a kategorizace informačních aktiv z hlediska jejich vazby na možné dopady.

Podrobnější návod k řízení bezpečnosti najdeme pouze ve vyhlášce č. 82/2018 Sb. (VoKB), která se však týká jen správců a provozovatelů systémů pod **zákonem o kybernetické bezpečnosti** (ZoKB č. 181/2014 Sb.). Vzhledem k velkému rozsahu dnes využívaných IS v různých úrovních organizací veřejné správy by bylo nereálné snažit se zavést jedno „minimum“ standardů zabezpečení, byť jen v té části IS, které nespadají do regulace ZoKB. Je třeba od začátku prosazovat tzv. „přístup založený na riziku“, a zavést odstupňované požadavky na bezpečnost IS v závislosti na hodnocení dopadů ztráty důvěrnosti, integrity a dostupnosti dat nebo služeb IT v IS. Toto hodnocení dopadů se týká primárně aplikační vrstvy IS, avšak promítá se i do technologické a komunikační vrstvy služeb dle skutečné funkční závislosti. Navrhujeme proto pracovat s pojmy „hodnocení dopadů ztráty důvěrnosti, integrity a dostupnosti IS nebo dekomponovaných ICT služeb“, zařadit tyto dopady do určitých úrovní, a od nich odvíjet požadavky na bezpečnostní úroveň příslušných ICT služeb.

Tento postup je v souladu s požadavky **obecného nařízení GDPR**, které zdůrazňuje přístup založený na riziku a posuzování vhodné úrovně bezpečnosti s ohledem na zpracování osobních údajů (viz čl. 32 bod 2. a další). Rizika spojená se zpracováním osobních údajů mohou představovat jedny z možných, zde hodnocených dopadů. Vazba na GDPR se promítne i ve stanovení požadavků na zpracovatele – poskytovatele cloudových služeb v rámci eGC, a to respektováním požadavků uvedených v čl. 28 „Zpracovatel“.

Tento postup je rovněž (na horním konci škály dopadů IS) v souladu s principy hodnocení rizik a kategorizace aktiv dle již zmíněné VoKB – příloha č. 1 a č. 2. Naším cílem je zavést jednodušší pravidla řízení bezpečnosti pro IS než jsou ZoKB a VoKB, avšak být s těmito pravidly kompatibilní v případech, kdy IS spadnou do rozsahu působnosti ZoKB.

4 Celkový koncept eGC

4.1 Slovníček pojmů eGC

Slovníček definuje základní pojmy a zkratky, často používané v dokumentu.

Zákazníci eGC. Tento dokument používá pro zjednodušení pro označení všech organizací, které mohou být zákazníky eGC, termín Zákazníci eGC. To dle definice v kapitole 5.1.1 zahrnuje orgány veřejné moci, orgány státní správy, orgány územních samosprávních celků, ale i podniky, ve kterých má stát alespoň 50% podíl.

Orgány veřejné moci (OVM) ve smyslu zákona č. 111/2009 Sb. (o základních registrech) zahrnují státní orgány, územní samosprávné celky a fyzické nebo právnické osoby, byla-li jim svěřena působnost v oblasti veřejné správy

Orgány veřejné správy (OVS) ve smyslu zákona č. 365/2000 Sb. (ZoISVS) zahrnují orgány státní správy a orgány územních samosprávných celků.

Orgány státní správy (OSS) zastupují stát a jsou zřizovány ústavou nebo zákonem, zejména zákonem č. 2/1969 Sb. (Kompetenční zákon).

Informační systém (IS). Tento dokument používá pro zjednodušení pro všechny informační systémy spravované (potenciálními) zákazníky eGC, tedy pro ISVS i pro provozní informační systémy, termín IS.

Informační systém veřejné správy (ISVS) ve smyslu zákona č. 365/2000 Sb. je funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy.

Provozní informační systém ve smyslu zákona č. 365/2000 Sb. je IS spravovaný pro jiný účel, než je výkon veřejné správy, tedy např. podpůrné systémy.

Hodnocení bezpečnostních dopadů IS je proces vyhodnocení závažnosti dopadů narušení dostupnosti, důvěrnosti a integrity dat nebo celé ICT služby, na kterých je funkčnost hodnoceného IS závislá. Tyto dopady se hodnotí v 9 oblastech, na stupnici 1-4 závažnosti dopadů (Nízká, Střední, Vysoká, Kritická), a to na základě metodiky popsané v kapitole 5.2. Tato metodika popisuje i mapování závažnosti dopadů na vhodnou bezpečnostní úroveň použitých služeb eGC (viz dále).

Bezpečnostní úroveň služeb eGC na stupnici 1-4 (Nízká, Střední, Vysoká, Kritická) je kategorizace úrovně bezpečnostních opatření služeb eGC, popsaná v kapitolách 5.2 a 6.2.

Hodnocení TCO (Total Cost of Ownership) je proces hodnocení celkových nákladů na vlastnictví produktu nebo služby (celkové náklady životního cyklu). Prostřednictvím TCO se vyjadřují kompletní náklady na investici a její provoz, zohledňující nejen pořizovací cenu, ale také výdaje vznikající vlastnictvím hodnocených statků. Pro případ eGC se prostřednictvím TCO hodnotí náklady na provoz služby ve státní, resp. komerční části cloudu.

Cloudové služby (cloud computing) je obecný technický termín označující ICT prostředky (výpočetní zdroje, úložiště, aplikace) a související služby poskytované typicky vzdáleně prostřednictvím komunikačních sítí jako služba externího poskytovatele s definovanými parametry kvality, realizovaná na sdílených platformách pro více uživatelů (multi-tenant). Dalšími typickými znaky cloudových služeb jsou vysoká míra flexibility a dynamického škálování alokovaných prostředků.

Cloud computing ve smyslu zákona č. 181/2014 Sb. Umožňuje přístup k rozšiřitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet.

IaaS služby (Infrastructure as a Service - infrastruktura jako služba) je pronájmem/poskytováním virtuálních HW zdrojů. Samostatnou součástí IaaS služeb na nejnižší úrovni jsou služby **housingu** (pronájmu prostoru v datovém centru spolu s odběrem elektřiny a síťovou konektivitou) pro umístění vlastního HW - někdy hovoříme též o službách typu **DCaaS (Data Center as a Service)**.

PaaS (Platform as a Service - platforma jako služba). Poskytování/pronájem výpočetní infrastruktury spolu se standardními SW platformami jako jsou operační systémy, databáze, webové a aplikační servery.

SaaS (Software as a Service - software jako služba). Poskytování/pronájem kompletní aplikační funkcionality jako služby dostupné po síti - kompletní funkcionalita standardních nebo standardizovatelných aplikací poskytovaná jako služba, např. e-mail, ekonomický systém, spisová služba apod.

eGovernment cloud ČR (eGC) je konkrétní systém cloudových služeb, definovaných, provozovaných a řízených v souladu s tímto dokumentem.

Služby eGC jsou cloudové služby eGovernment cloudu ČR uvedené v Katalogu služeb eGC.

Komerční část eGC (KeGC) jsou služby eGC provozované komerčními subjekty s využitím jejich vlastních datových center a komunikační infrastruktury. Komerční část eGC je určena pro provoz služeb eGC bezpečnostních úrovní 1-3 (Nízká, Střední, Vysoká).

Státní část eGC (SeGC) jsou služby eGC provozované v datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem (státní podniky) a v rámci provozu musí být ošetřená autorská práva třetích stran (za účelem zamezení vendor-locku). Státní část eGC zajistí maximální úroveň bezpečnosti a je určena pro provoz služeb eGC bezpečnostní úrovně 4 (Kritická).

Hybridní eGC je kombinací služeb KeGC a SeGC, která vychází z principu dekompozice IS na části s různými úrovněmi bezpečnostních dopadů. Hybridním eGC nazýváme scénář, kdy zákazník eGC zadá služby eGC pro provoz celého IS provozovateli SeGC, ve spolupráci s ním dekomponuje IS na části s požadovanou bezpečnostní úrovní 4 (Kritická) a části s nižšími bezpečnostními úrovněmi. Provozovatel SeGC pak sám provozuje části IS s bezpečnostní úrovní 4 (Kritická) a pro ostatní části vybere (vysoutěží) provozovatele KeGC.

Katalog služeb eGC je seznam služeb eGC, který definuje služby eGC, jejich strukturu a hierarchii a jejich parametry.

Katalogový list služby eGC je popis jedné služby, určuje zejména parametry, kterými je daná služba definována.

Vzhledem k použitým soutěžním a nákupním mechanismům KeGC je katalog služeb eGC ve skutečnosti tvořen sadou souvisejících katalogů s jednotnou strukturou:

- **Rámcový katalog služeb eGC** – popisuje strukturu a hierarchii služeb eGC, jejich povinné parametry, minimální smluvní podmínky a další související informace. Slouží zároveň jako primární společná struktura služeb pro všechny ostatní katalogy KeGC i SeGC. Je vytvořen a udržován ŘOeGC.
- **Katalog tržní nabídky služeb KeGC** obsahuje obecné nabídky dodavatelů KeGC, včetně detailních parametrů služby a indikativních cen. Strukturu katalogu a strukturu parametrů služeb určuje ŘOeGC, jeho obsah naplňují potenciální dodavatelé KeGC.
- **Katalog poptávek služeb KeGC** obsahuje konkrétní zadání minitendrů soutěžního

mechanismu KeGC. Jednotlivá zadání jsou tvořena zákazníky eGC. • **Katalog závazných nabídek služeb KeGC** obsahuje závazné nabídky dodavatelů KeGC včetně cen, odpovědí na poptávky služeb eGC v jednotlivých minitendrech. • **Katalog služeb SeGC** obsahuje seznam a popis detailně definovaných, přímo objednatelných služeb eGC, vytvořený provozovatelem SeGC ve spolupráci a pod kontrolou ŘOeGC.
Státní ICT podniky – státní podniky, založené jednotlivými resorty pro poskytování ICT služeb v rámci resortu (SPCSS, NAKIT, CENDIS).
Řídící orgán eGC (ŘOeGC) ŘOeGC je Řídící orgán eGC (viz obdoba Government Digital Service ve Velké Británii nebo Úradu podpredsedu vlády SR pre investície a informatizáciu na Slovensku). ŘOeGC řídí rozvoj a provoz státní i komerční částí eGC. ŘOeGC zřídí ministr vnitra jako nový útvar v rámci MV ČR. Pro ŘOeGC bude zřízen meziresortní poradní orgán složený ze zástupců Ministerstva vnitra, Ministerstva financí a NÚKIB, zástupců zpravodajských služeb, zástupců ústředních orgánů státní správy, zástupců orgánů veřejné správy a zástupců odborné veřejnosti.
OHA - odbor Hlavního architekta eGovernmentu Ministerstva Vnitra
SLA - Service Level Agreement – Smlouva o úrovni poskytovaných služeb (součást smlouvy o poskytování služeb eGC)
Migrace IS do eGC Projekt *Příprava vybudování eGC* nabízí a zpracovává dva základní pohledy na služby eGC a pravidla jejich použití. • Pohled využití služeb eGC v kontextu jednoho IS - nabídka standardizovaných služeb KeGC nebo SeGC, jejich bezpečnostní a provozní standardy a procesy usnadňující jejich využití. • Celkový koncepční pohled na proces migrace IS do eGC – plánování a sledování dlouhodobého postupného procesu umístění většiny IS veřejné správy do eGC, provádí ŘOeGC. • Pohled zákazníka eGC na proces migrace všech jeho IS do eGC - lokální obdoba procesu migrace do eGC, provádí zákazník eGC

4.2 Základní pravidla a principy eGC

a) Určení eGC služeb – ŘOeGC bude identifikovat identické nebo podobné ICT služby (typu IaaS, PaaS, SaaS) dosud provozované odděleně pro různé potenciální zákazníky eGC. Tyto služby budou postupně standardizovány (tj. budou stanoveny minimální požadavky na funkcionalitu, interoperabilitu, bezpečnost, dostupnost atd.) a standardizovaná služba bude nabízena pro více institucí současně z eGC. Standardizovaná služba bude v KeGC nabízena více poskytovateli (viz konkurence poskytovatelů KeGC dále).
b) Pro rozvoj a provoz služeb eGC platí jednotná pravidla určená OHA a ŘOeGC. Nová služba eGC nemůže být schválena (ověřena pro provoz v eGC), jestliže není s těmito pravidly v souladu.
c) U každého aktuálně provozovaného IS musí jeho **správce určit a nadále sledovat plánované i skutečné investiční a provozní náklady** a dále požadavky na objem (počet uživatelů apod.) a kvalitu (bezpečnostní úroveň, SLA) ICT služeb v rámci IS. Metodika pro sledování a porovnávání TCO služeb (on-premise i cloudových) musí být závazná a vymahatelná.
d) eGovernment Cloud (eGC) se skládá ze dvou částí – Státní části (SeGC) a Komerční části (KeGC).
e) Ve státní části eGC budou provozovány ty služby eGC, na něž jsou kladeny nejvyšší bezpečnostní požadavky (bezpečnostní úroveň 4 - Kritická). Všechny ostatní služby budou poskytovány **Komerční částí eGC.**
f) Provozovatelé SeGC si nebudou konkurovat mezi sebou, ani s provozovateli KeGC. Cílem je maximalizovat využití zdrojů státních datových center a zajistit efektivitu vložených finančních prostředků a současně se vyhnout možným obviněním státu za nedovolenou podporu v konkurenčním boji.
g) Provozovatelé KeGC si budou mezi sebou konkurovat, tzn. že ŘOeGC bude při řízení KeGC postupovat tak, aby každý typ služby eGC byl z KeGC nabízen více provozovateli. Cílem je vyhnout se „vendor lock-in“ a zajistit konkurenční tržní prostředí.
h) SeGC poskytuje služby, které nelze poskytovat v KeGC, proto jeho zákazníci (zákazníci SeGC) objednávají jeho služby **bez potřeby veřejné zakázky**.
i) Na nákup služeb **KeGC jsou aplikována pravidla ZZVZ** (Dynamický nákupní systém – DNS).
j) Služby SeGC i KeGC jsou nabízeny jednotlivým zákazníkům eGC prostřednictvím **Portálu eGC**. Zákazníci eGC pomocí tohoto portálu služby eGC vybírají a v ideálním případě i nakupují.
k) Zákazníci SeGC i KeGC **uzavírají s vybraným provozovatelem služeb smlouvu** o **poskytování služeb**, jejíž součástí je i definice SLA. Za **užívání služeb SeGC i KeGC zákazníci eGC platí**.
l) Za porušení SLA je provozovatel služby penalizován.
m) Smlouva o poskytování služeb KeGC bude vždy obsahovat jasnou **možnost ukončení**

služby a podporu přechodu k jinému provozovateli služby (vč. podpory migrace dat).

n) Umístění IS do eGC je **dobrovolné pro**

- kraje, města, obce,
- ČNB,
- zpravodajské služby,
- systémy bezpečnostních sborů, pokud provoz těchto systémů souvisí s plněním zákonem jim stanovených úkolů,
- systémy orgánů činných v trestním nebo soudním řízení, pokud provoz těchto systémů slouží pro trestní nebo soudní řízení,
- systémy v oblasti národní bezpečnosti,
- právnické osoby, v nichž má stát podíl alespoň 50%.

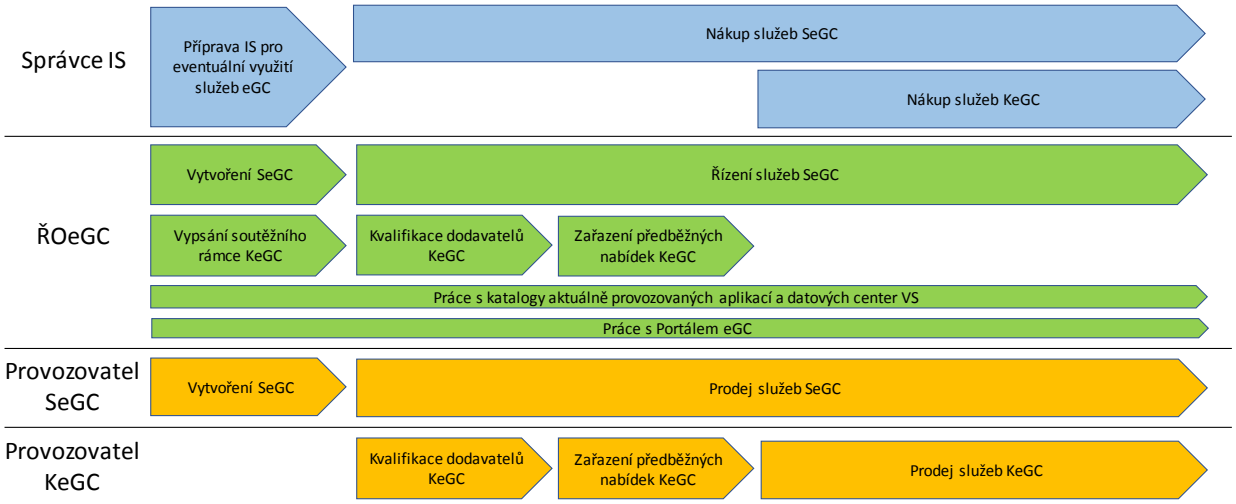
Pro OSS a jejich IS bude v první fázi (cca 2 roky) využití služeb eGC také dobrovolné. Po schválení příslušné legislativy bude pro OSS a jejich IS neuvedené výše uplatněn princip **cloud first**, tj. jestliže dožije technologická infrastruktura stávajícího informačního systému nebo se staví nový či inovovaný informační systém, pak:

- Zákazník eGC musí využít služby eGC nejvyšší úrovně (prioritně SaaS, pak PaaS, nakonec IaaS), které naplňují potřeby části nebo celého IS.
- Umístění do eGC je nepovinné tehdy, když správce IS na základě analýzy TCO prokáže ekonomickou výhodnost jiného řešení.

4.3 Procesy eGC – hrubý pohled dle aktérů

Následující kapitoly obsahují celkový procesní pohled na eGC, průřezový a přehledový vzhledem k ostatním kapitolám.

Následující obrázek znázorňuje všechny hlavní procesy eGC dle jednotlivých aktérů a časové návaznosti těchto procesů.



Poznámka: *Tato kapitola (a ostatní kapitoly mimo kapitoly 7) využívá pro odkazy na soutěžní mechanismus KeGC obecnou terminologii (soutěžní rámec, kvalifikace, minitendr, zadání, tržní nabídka, poptávka, nabídka, závazná nabídka, …) bez přímé konkrétní vazby na terminologii a mechanismy ZZVZ. Cílem je popsat používané soutěžní mechanismy z procesního pohledu. Vazba na konkrétní mechanismy a terminologii ZZVZ je popsána v kapitole 7.*

4.4 Procesy správce IS

4.4.1 Příprava IS pro eventuální využití služeb eGC

Proces společný pro SeGC a KeGC

Věcný správce IS:

- s pomocí metodik eGC zhodnotí pro svůj IS závažnost bezpečnostních dopadů a pro celý IS nebo pro jeho jednotlivé funkční části stanoví úroveň bezpečnostních dopadů 1-4 (Nízká, Střední, Vysoká, Kritická),
- identifikuje další služby (monitoring, service desk, penetrační testy, dočasné datové úložiště, služby mobilního sdílení dat, služby osobní produktivity, služby správy koncových uživatelských zařízení, služby portálu jako end user interface, provozní personál, konzultační služby, atd. ...), které k provozu a rozvoji IS potřebuje,
- stanoví odpovídající architekturu implementace IS s využitím služeb eGC,
- s pomocí TCO metodiky eGC určí části IS, pro jejichž provoz by bylo ekonomické využít služeb eGC,
- uloží do ISoISVS (tj. Do katalogu aktuálně provozovaných IS) informace o svém IS v požadované struktuře, včetně případného požadavku na využití služeb eGC.

Svoje údaje v ISoISVS musejí věcní správci minimálně jedenkrát ročně aktualizovat.

ŘOeGC pravidelně (minimálně 1x ročně) kontroluje plnění a změny katalogu aktuálně provozovaných IS. V případě, že s některými údaji nesouhlasí (to se týká zejména údajů TCO a údaje o zařazení komponenty do jedné ze čtyř úrovní požadované bezpečnosti), projedná tyto údaje se správcem. Případné neshody řeší ŘOeGC s pomocí svého poradního orgánu a v další instanci ministr vnitra s příslušným ministrem nebo statutárním zástupcem příslušného ústředního orgánu.

4.5 Procesy SeGC

4.5.1 Vytvoření SeGC

Ve státní části eGC budou poskytovány služby eGC, které byly zařazeny do bezpečnostní úrovně 4 (Kritická).

Právní rámec SeGC bude zvolen na základě legislativního rozboru variant a doporučení meziresortní komise garantů jednotlivých relevantních zákonů – MV (ZoISVS), MF (ZoRP), MPO (ZoSP) a MMR (ZZVZ) – ve spolupráci s pracovní skupinou RVIS pro přípravu vybudování eGovernment cloudu na základě požadavků, kritérií a variant uvedených v tomto dokumentu, do 30.6.2019. *Právní rámec SeGC je popsán v kapitole 8, bezpečnostní a provozní požadavky, které musí SeGC splňovat, jsou popsány v kapitole 6.*

Služby SeGC budou součástí katalogu služeb eGC a budou popisovány jednotnými parametry platnými pro všechny služby eGC.

Po zvolení právního rámce SeGC, přípravě a schválení legislativních změn, zřízení poskytovatele SeGC, přípravě jeho katalogu služeb eGC a ověření katalogu i naplnění bezpečnostních a provozních požadavků ze strany ŘOeGC budou moci všechny OSS využívat služeb SeGC napřímo (tj. Na základě výjimky ze ZZVZ).

4.5.2 Řízení služeb SeGC

ŘOeGC:

- prověří a schválí požadavky věcných správců IS na využití služeb SeGC v jednotlivých časových obdobích. Tyto požadavky na využití služeb SeGC musí být podloženy zařazením do bezpečnostní úrovně 4 (Kritická) dle metodiky hodnocení závažnosti bezpečnostních dopadů (viz kapitoly 5.2 a 6.2). Případné rozpory mezi správcem IS a ŘOeGC řeší ŘOeGC s pomocí svého poradního orgánu a v další instanci ministr vnitra s příslušným ministrem nebo statutárním zástupcem příslušného ústředního orgánu,
- na základě schválených požadavků určí potřebnou kapacitu služeb SeGC v jednotlivých časových obdobích. při této činnosti ŘOeGC postupuje tak, aby optimálně využil stávající zdroje SeGC a současně aby pokryl pokud možno všechny požadavky OSS na využití služeb SeGC,
- ověří naplnění bezpečnostních a provozních požadavků provozovatelem SeGC v dané etapě, a to ve spolupráci s NÚKIB,
- dohodne s provozovatelem SeGC nabídkové parametry služeb SeGC (zejména vzorová SLA a jednotkové nabídkové ceny). Poté služby zveřejní na portálu eGC, a to ve stejné struktuře jakou mají katalogy služeb KeGC,
- vytvoří harmonogram pro migraci IS do SeGC – ten bude vytvořen na základě těchto typů informací získaných z katalogu DC a z katalogu ISoISVS,
- kdy bude ukončena životnost DC, ve kterém je IS aktuálně provozován,
- jak velký je rozdíl mezi požadovanou úrovní bezpečnosti daného IS a úrovní, které je schopno zajistit stávající DC (čím větší tento rozdíl bude, tím vyšší bude priorita migrace IS do SeGC),

- na jaké platformě je IS provozován,
- jaký je plánovaný rozvoj IS,
- jaké jsou volné kapacity SeGC,
- monitoruje migraci IS do SeGC a monitoruje provoz služeb SeGC.

4.5.3 Nákup služeb SeGC

Věcný správce IS:

- Na základě katalogu služeb SeGC dohodne s provozovatelem SeGC poskytované služby a uzavře smlouvu.

Další kroky (zprovoznění služeb SeGC, užití služeb SeGC, ukončení služby SeGC) probíhají obdobně jako v KeGC.

4.6 Procesy KeGC

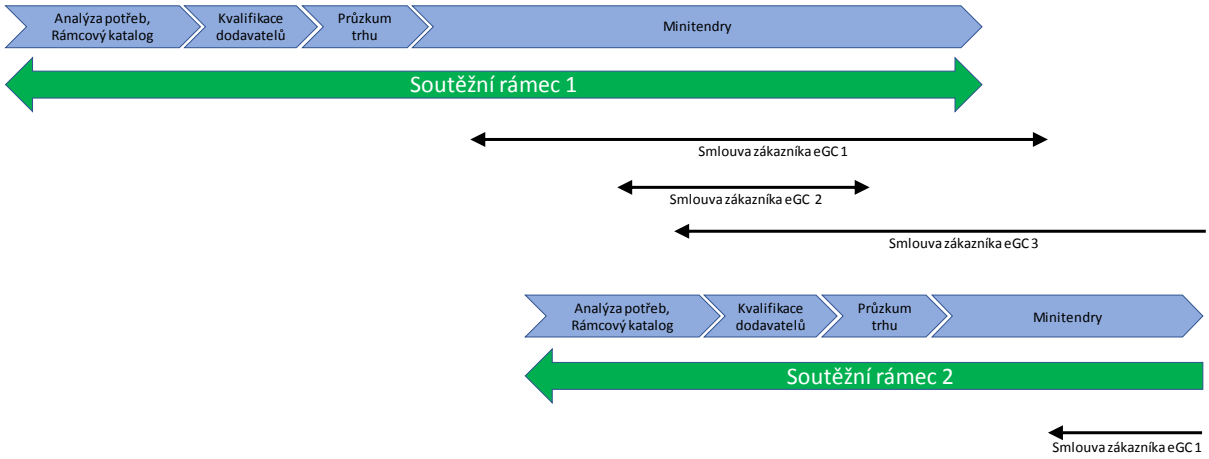
Inspirací pro procesy KeGC jsou osvědčené praktiky Velké Británie a Dánska s fungováním government cloudu.

Tato kapitola poskytuje základní procesní přehled, detailní popis jednotlivých mechanismů je v kapitole 5.5 a 5.4.

Pro nákup služeb z KeGC se využívá dvoustupňový soutěžní mechanismus s centrálním zadáváním. Mechanismus musí umožňovat průběžné zapojování dalších zadavatelů (zákazníků KeGC) a dodavatelů/provozovatelů služeb eGC.

Soutěžní mechanismus KeGC je organizován v pevně daných, obsahově a časově vymezených **soutěžních rámcích** (viz obrázek). Soutěžní rámce se mohou časově překrývat a mohou v nich platit různá pravidla. Katalog služeb eGC bude realizován rozdělením do několika paralelních soutěžních rámců podle typu služby (nap. oddělení IaaS/PaaS a SaaS) nebo podle bezpečnostních úrovní.

Soutěžní rámce a jejich pravidla vypisuje ŘOeGC.



V případě, že praxe ukáže, že jak pro dodavatele, tak pro ŘOeGC bude efektivnější organizačně spojit či jinak kombinovat krok kvalifikace dodavatelů do soutěžního rámce s průzkumem trhu za účelem získání informace o tržní nabídce, tj. Např. že dodavatel odpoví na kvalifikační požadavky a současně připojí odpověď na průzkum trhu, může ŘOeGC proces popsaný v tomto dokumentu příslušně upravit.

4.6.1 Vypsání soutěžního rámce KeGC

ŘOeGC:

- provede analýzu aktuálních potřeb (potenciálních) zákazníků eGC, která zjistí, jaké ICT služby jsou jednotlivými organizacemi provozovány a požadovány a jaké z nich realizací v eGC přinesou největší efekt. Současně zohlední stav a vývoj technologických možností nových cloudových služeb. při analýze využívá katalog aktuálně provozovaných IS (ISoISVS),
- na základě výsledků analýzy ŘOeGC vytvoří a na Portálu eGC publikuje novou verzi Rámcového katalogu eGC nebo jeho části, která je zadáním předmětu soutěžního rámce. Požadavky na každou službu eGC jsou popsány v katalogovém listu eGC řadou parametrů. Některé parametry mají povinný charakter a jsou předmětem kvalifikace dodavatelů KeGC v daném soutěžním rámci,
- definuje další kvalifikační podmínky soutěžního rámce, včetně požadavků na bezpečnostní úrovně,
- formuluje předmět a kvalifikaci soutěžního rámce tak, aby nabídku daného typu služby mohlo podat více potenciálních dodavatelů,
- ve spolupráci s OVZ MV vypíše soutěžní rámec.

4.6.2 Kvalifikace dodavatelů do soutěžního rámce KeGC

Potenciální dodavatelé KeGC:

- registrují se do Portálu eGC, pokud již nejsou registrováni. V případě, že se dodavatel účastní více soutěžních rámců, využívá pro všechny stejný účet na Portálu eGC,
- odpoví na kvalifikační podmínky soutěžního rámce.

ŘOeGC (ve spolupráci s MV):

- posoudí odpovědi potenciálních dodavatelů a zařadí do soutěžního rámce ty, kteří splňují kvalifikační podmínky.

Kvalifikace nových dodavatelů do soutěžního rámce je možná kdykoliv v průběhu trvání soutěžního rámce.

4.6.3 Zařazení informací do Katalogu tržní nabídky služeb KeGC

ŘOeGC:

- vyzve formou průzkumu trhu kvalifikované dodavatele k předložení nebo aktualizaci informací o jejich poskytovaných službách eGC.

Kvalifikovaný dodavatel:

- (nepovinně) poskytne popis poskytovaných služeb eGC odpovídajících sadě služeb Rámcového katalogu eGC, která je předmětem soutěžního rámce. Popis je poskytován ve standardizované podobě pro zařazení do Katalogu tržní nabídky KeGC.

ŘOeGC:

- posoudí předložené informace, zda odpovídají předmětu a dalším podmínkám soutěžního rámce,
- zařadí popisy vyhovujících služeb do Katalogu tržní nabídky služeb KeGC a publikuje je na Portálu eGC.

ŘOeGC umožní po celou dobu trvání soutěžního rámce dodavateli aktualizovat informace o poskytovaných službách, a to za předpokladu, že zůstane nadále v souladu s předmětem a dalšími podmínkami soutěžního rámce.

4.6.4 Nákup služeb KeGC orgánem veřejné moci (minitendr)

ŘOeGC

- stanovuje metodiku a pravidla nákupního systému,
- vytváří nástroje (v rámci Portálu eGC) pro zjednodušení tvorby zadání minitendru a pro porovnání a výběr nejvhodnější nabídky,
- koordinuje případné sdružení více minitendrů stejného obsahu do jednoho minitendru většího rozsahu za účelem získání výhodnějších nákupních cen (za podmínky souhlasu zúčastněných zákazníků eGC),
- zveřejní poptávku a přijaté nabídky, včetně označení vítězné nabídky (smlouvy) v Katalogu poptávek a nabídek KeGC.

Správce IS (zákazník eGC):

- na základě informací uložených v Katalogu tržní nabídky KeGC a v Katalogu poptávek KeGC a Katalogu nabídek KeGC a na základě požadavků a specifických podmínek zákazník eGC připraví zadání minitendru. Předmět minitendru má formu katalogových listů jednotlivých služeb KeGC v jednotné formě (sada parametrů), které rozvíjí a doplňují katalogové listy Rámcového katalogu eGC o specifické požadavky zákazníka eGC. Může rozšířit skupinu povinných parametrů a určit parametry hodnotící, které budou předmětem hodnocení nabídek,
- formuluje zadání minitendru tak, aby nebylo diskriminující a aby nabídku mohlo podat více potenciálních dodavatelů,
- zveřejní zadání v Katalogu poptávek KeGC na Portálu eGC,
- může pro expertní pomoc při realizaci minitendru nakoupit konzultační služby, rovněž prostřednictvím eGC. SeGC poskytuje konzultační služby pro bezpečnostní úroveň 4 (Kritická) a služby Hybridního eGC, KeGC (samostatný soutěžní rámec) pro bezpečnostní úrovně 1-3 (Nízká, Střední, Vysoká). Tyto služby zahrnují zejména: návrh řešení s využitím služeb eGC, hodnocení závažnosti bezpečnostních dopadů a stanovení požadované úrovně bezpečnosti, výpočet TCO a příprava zadání minitendru.

V případě, že zákazník eGC alternativně uvažuje o využití on-premise řešení nebo externího řešení mimo eGC, spočítá pro alternativní řešení TCO dle standardní metodiky eGC.

Kvalifikovaní dodavatelé:

- mohou ve lhůtě určené zadavatelem minitendru podat prostřednictvím portálu eGC své závazné nabídky do minitendru.

Správce IS (zákazník eGC):

- ohodnotí přijaté nabídky a vybere dodavatele,
- uzavře smlouvu s dodavatelem.

4.6.5 Implementace služby KeGC

- Provedení implementační nebo migrační fáze (pokud je potřeba).
- Nastavení a zprovoznění provozní dokumentace služby a monitoringu služby.
- Zprovoznění služby.

4.6.6 Provoz služby KeGC

- Poskytování služby uživatelům.
- Monitoring služby.
- Řešení mimořádných stavů (incidentů).
- Řešení změn smlouvy.
- Placení za službu.

4.6.7 Ukončení služby KeGC

K ukončení služby KeGC může dojít z několika příčin:

- na základě smluvně validního rozhodnutí zákazníka eGC (tato možnost musí být uvedena v popisu služby katalogu KeGC),
- na základě hrubého neplnění SLA poskytovatelem,
- na základě uplynutí doby platnosti smlouvy.

Kontrola korektního ukončení služby

- Zpětný převod dat a bezpečné smazání dat z úložišť poskytovatele (v souladu s požadavky vyhlášky č. 82/2018 Sb. V aktuálním znění).

Kontrola splnění všech ostatních požadovaných provozních parametrů ukončení služby včetně podpory migrace k jinému provozovateli, předání dat, instalace aplikací, dokumentace apod.

4.7 Podpůrné procesy řízení eGC

4.7.1 Práce s katalogy aktuálně provozovaných IS a datových center veřejné správy

ŘOeGC ve spolupráci s dalšími útvary MV zajistí **úpravu stávajícího ISoISVS včetně vytvoření funkcionality pro správu katalogu datových center veřejné správy** tak, aby ISoISVS byl schopen uchovávat informace potřebné pro řízení eGC (viz příloha č. 2 *Katalog aktuálně provozovaných IS*).

Poznámka: V rámci stávající i připravované novely zákona č. 111/2009 Sb., o základních registrech, dochází k postupnému přesunu datového fondu ISoISVS do Registru práv a povinností (RPP) a dále se zavádí katalog úkonů na žádost (katalog podání, katalog služeb VS). Příloha č. 2 *Katalog aktuálně provozovaných IS* je sadou požadavků ze strany eGC na funkcionalitu těchto systémů a bude aktualizována ŘOeGC na základě vývoje ISoISVS a RPP.

ŘOeGC zajistí propojení Katalogu aktuálně provozovaných IS s katalogem SaaS služeb eGC.

Správci IS udržují aktuální informace o svém IS v katalogu, viz proces Příprava IS pro eventuální využití eGC (kapitola 4.4.1).

ŘOeGC využívá údaje v katalogu pro:

- určování vhodných kandidátů na sdílené služby eGC a k vypisování soutěžních rámců KeGC,
- plánování potřebných kapacit SeGC,
- stanovování harmonogramu migrace IS do SeGC,
- analýzu změn indikovaných bezpečnostních úrovní provozovaných IS (přesun do eGC zajišťuje bezpečné prostředí provozu daného IS),
- analýzu investičních a provozních nákladů provozovaných IS a jejich změn vyvolaných provozováním eGC,
- analýzu podílu služeb eGC na všech ICT službách VS.

Správci IS uloží a budou udržovat aktuální informace o datových centrech, ve kterých jsou umístěny jejich IS v katalogu datových center veřejné správy, a to včetně informací o jejich kapacitě a o bezpečnostní úrovni (dle metodiky eGC), kterou jsou ve stávajícím datovém centru schopni garantovat.

Svoje údaje v katalogu musejí správci IS minimálně jedenkrát ročně aktualizovat.

ŘOeGC využívá údaje v katalogu datových center veřejné správy jednak při vytipovávání případných kandidátů pro zařazení do SeGC a jednak pro stanovování harmonogramu migrace IS do SeGC.

4.7.2 Práce s Portálem eGC

ŘOeGC zajistí **vytvoření a údržbu Portálu eGC**, tak, aby vhodně podporoval řízení eGC a využívání eGC pro jednotlivé typy uživatelů portálu:

pro ŘOeGC:

- správa a zveřejňování katalogů služeb eGC,
- vypisování a správu soutěžních rámců pro KeGC,
- monitorování stavu provozu eGC.

pro provozovatele služeb KeGC:

- registraci dodavatele a správu informací o tržní nabídce,
- v dlouhodobém horizontu i jako nástroj pro podávání nabídek do minitendrů.

pro zákazníky služeb KeGC:

- analýza vhodných služeb KeGC pro daného zákazníka eGC,
- příprava zadání minitendru KeGC,
- v dlouhodobém horizontu i výběr nejvhodnějšího dodavatele poptávaných služeb KeGC,
- uložení poptávky, závazných nabídek a smlouvy v katalozích KeGC.

pro dodavatele služeb SeGC:

- uložení nabídky služeb SeGC.

pro zákazníky služeb SeGC:

- analýza vhodných služeb SeGC pro daného zákazníka eGC,
- výběr vhodných služeb SeGC,
- uložení smlouvy v Katalogu služeb SeGC.

5 Pohled správce IS – zákazníka eGC

Tato kapitola popisuje koncepty a procesy eGC z pohledu jeho zákazníků - integruje pohledy na KeGC a SeGC, které zároveň definuje. Kapitola zároveň uvádí řadu definic a témat společných pro celý dokument.

5.1 Umísťování IS do eGC

5.1.1 Zákazníci eGC

Z pohledu organizačního jsou zákazníky eGC (tedy organizacemi, které mohou využívat eGC) všechny orgány veřejné moci (OVM), tj.

- organizační složky státu (OSS),
- orgány územních samospráv, tj. krajů, měst a obcí.

a právnické osoby, v nichž má stát podíl alespoň 50%.

Tento dokument používá pro zjednodušení pro označení všech organizací, které mohou být uživateli eGC, termín **zákazníci eGC**.

Zákazníci eGC mohou využívat eGC pro potřeby všech spravovaných informačních systémů. Tento dokument používá pro zjednodušení pro všechny informační systémy spravované zákazníky eGC, tedy i pro provozní informační systémy, termín **IS**.

Z pohledu provozního a procesního je zákazníkem eGC vždy správce IS (zobecnění role správce ISVS dle ZoISVS).

5.1.2 Pravidla umísťování do eGC

Pravidla umísťování do eGC (využívání služeb eGC) se vztahují na veškeré informační systémy, provozované výše uvedenými organizacemi, tj. ISVS a provozní IS regulované dle ZoISVS, i další provozní a interní informační systémy. Pravidla umísťování do eGC jsou formulována vždy z pohledu jednoho IS.

Formulace pravidel umísťování využívá termíny a odkazy na metodiky definované a vysvětlené v následujících kapitolách.

Ve Fázi II. (pilotní), dočasného období zhruba 2 roky, bude využívání služeb eGC dobrovolné pro všechny potenciální zákazníky eGC. Možnost umísťování do státní části eGC bude v této fázi dále podmíněna zvoleným právním rámcem (viz kapitola 8).

Ve Fázi III. (standardizační), po ukončení přípravy a schválení souvisejících legislativních změn, budou aplikována následující pravidla:

Umístění IS do eGC je **dobrovolné pro**

- kraje, města, obce,
- ČNB,
- zpravodajské služby,
- systémy bezpečnostních sborů a zpravodajských služeb, pokud provoz těchto systémů souvisí s plněním zákonem jim stanovených úkolů,
- systémy orgánů činných v trestním nebo soudním řízení, pokud provoz těchto systémů slouží pro trestní nebo soudní řízení,
- systémy v oblasti národní bezpečnosti,
- právnické osoby, v nichž má stát podíl alespoň 50%.

Umístění IS do eGC pro **organizační složky státu (OSS) neuvedené v předchozím seznamu** bude v této fázi řízeno na základě principu **„cloud first“,** konkrétně.:

a) Pokud v nabídce eGC existují služby typu SaaS, které naplňují potřeby části nebo celého IS, musí správce IS za dále uvedených podmínek (viz bod c) využít vhodnou kombinaci služeb eGC typu SaaS, pokrývající maximální rozsah potřeb daného IS.

b) Pro oblasti IS, které nepokrývá žádná existující eGC služba typu SaaS, musí správce IS za dále uvedených podmínek (viz bod c) využít služby PaaS (preferovaná varianta), resp. IaaS, v rozsahu potřeb daného IS.

c) Umístění do eGC je nepovinné tehdy, když správce IS na základě analýzy TCO prokáže ekonomickou výhodnost jiného řešení.

Při uplatnění uvedených pravidel umísťování do eGC budou zohledněny termíny udržitelnosti stávajících investic do technologické infrastruktury, termíny udržitelnosti z hlediska čerpaných dotací EU a termíny obnovy nebo významného rozšíření technologické infrastruktury stávajících IS. Stávající IS, resp. jejich části tedy budou umístěny do eGC až v momentě „dožití“ infrastruktury, na které jsou provozovány. Jde o tzv. „nenásilnou“ formu migrace, aby byly efektivně využity již investované finanční prostředky.

Analýza TCO bude provedena s využitím metodiky kalkulace TCO stanovené pro eGC (viz dále). Předpokladem pro analýzu a srovnání TCO různých řešení je naplnění bezpečnostních, provozních a architektonických požadavků odpovídajících požadavkům na provozovatele eGC (viz kapitola 6) pro danou bezpečnostní úroveň dle hodnocení bezpečnostních dopadů daného IS. Kalkulace TCO umožňuje zahrnutí nákladů na uvedení on-premise prostředí do souladu s bezpečnostními požadavky. Stejně tak TCO kalkulace umožňuje zahrnutí migračních a případně i reimplementačních nákladů při migraci do eGC (viz nákladové položky označené „Náklady na zavedení a změnu ICT služby“).

Z pohledu **umístění do státní nebo komerční části eGC** (pravidla platná pro Fázi II. i Fázi III.):

- IS nebo jejich části s požadovanou bezpečnostní úrovní 4 (Kritická) budou umísťovány do státní části eGC.
- IS nebo jejich části s požadovanou bezpečnostní úrovní 1-3 (Nízká, Střední, Vysoká) budou umísťovány do komerční části eGC.

V závislosti na zvolené variantě řešení právního rámce SeGC budou ve Fázi II. a Fázi III. seznam IS k umístění do státní části eGC a seznam výjimek z umístění IS bezpečnostní úrovně 4 (Kritická) do eGC určovány na základě pravidel uvedených v této kapitole zákonem nebo podzákonným předpisem.

Uvedená pravidla se nevztahují na IS zpracovávající utajované informace ve smyslu zákona č. 412/2005 Sb. o utajovaných informacích.

5.1.3 Komerční a státní část eGC

Komerční část eGC (KeGC) jsou služby eGC provozované komerčními subjekty s využitím jejich vlastních datových center a komunikační infrastruktury. Komerční část eGC je určena pro provoz služeb eGC bezpečnostních úrovní 1-3 (Nízká, Střední, Vysoká). Provozovatelé KeGC musí splnit bezpečnostní a provozní požadavky odpovídající těmto bezpečnostním úrovním služeb eGC. Zákazníci eGC nakupují služby provozovatelů KeGC na základě centralizovaného soutěžního mechanismu, který zajišťuje standardizaci služeb KeGC a optimální ceny.

V komerční části eGC budou již od počátku využívány všechny typy služeb eGC, tj. IaaS, PaaS, SaaS, služby systémové integrace a konzultační služby.

Státní část eGC (SeGC) jsou služby eGC provozované organizacemi v datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem (OSS nebo státní podniky) a v rámci provozu musí být ošetřená autorská práva třetích stran (zákaz vendor-locku). Státní část eGC zajistí maximální úroveň bezpečnosti a je určena pro provoz služeb eGC bezpečnostní úrovně 4 (Kritická). Zákazníci eGC využívají služby provozovatelů

SeGC prostřednictvím přímých smluvních vztahů (na základě výjimky ze ZZVZ). Provozovatelé SeGC podléhají plánovací a kontrolní činnosti ŘOeGC.

Ve státní části eGC budou zpočátku využívány především služby typu PaaS a IaaS, tzn., že stávající SW aplikace (např. agendový systém) bude migrován ze stávajícího datového centra a HW platforem zákazníka eGC do sdíleného DC a na sdílené HW platformy provozovatele SeGC.

Hybridní eGC je kombinací služeb KeGC a SeGC, která vychází z principu dekompozice IS na části s různými bezpečnostními dopady a požadavky na bezpečnostní úroveň služeb eGC - např. datová část IS (back-end) s nároky na bezpečnostní úroveň 4 (Kritická) vzhledem k dlouhodobému uložení dat a komunikační část IS (front-end, transakční část) s nižšími nároky na bezpečnostní úroveň 3 (Vysoká). V takovém případě může využít jednu ze dvou možností provozu IS v rámci eGC:

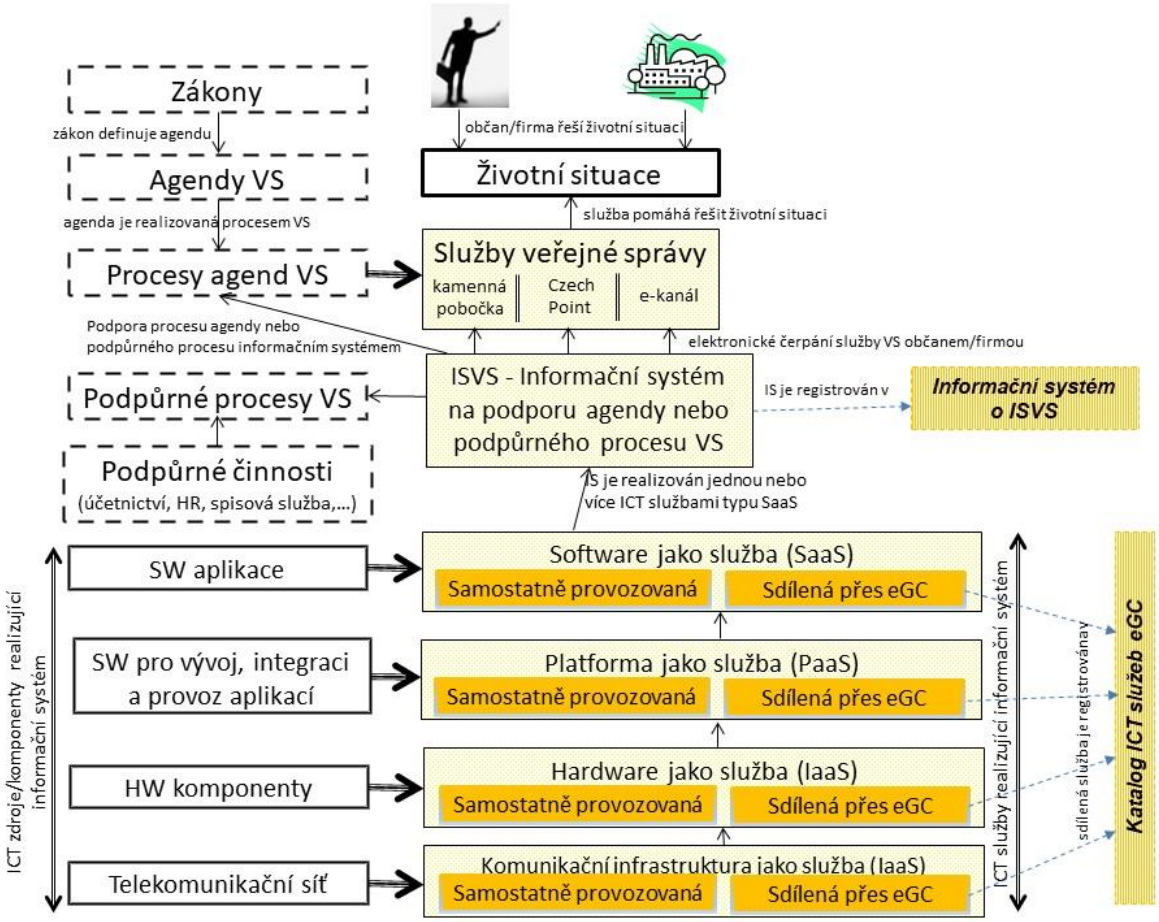
- zákazník eGC dekomponuje IS na část s bezpečnostní úrovní 4 (Kritická) a části s nižší bezpečnostní úrovní, jednotlivé části realizuje samostatně v SeGC a KeGC, integraci obou částí zajistí zákazník eGC,
- zákazník eGC zadá služby eGC pro provoz celého IS provozovateli SeGC. Ve spolupráci s ním dekomponuje IS na části s bezpečnostní úrovní 4 (Kritická) a části s nižší bezpečnostní úrovní. Provozovatel SeGC pak sám provozuje části IS s bezpečnostní úrovní 4 (Kritická) a pro ostatní části vybere (vysoutěží) provozovatele KeGC. Provozovatel SeGC zajistí integraci vlastních služeb se službami KeGC.

Hybridním eGC nazýváme druhý popisovaný scénář. Jde o variantu služeb SeGC, která poskytuje maximální komfort zákazníkovi eGC, a přitom zajistí optimální cenovou úroveň služeb. Provozovatel SeGC je v tomto scénáři zákazníkem KeGC.

5.1.4 Architektura IS s využitím služeb eGC

Využití služeb eGC v rámci IS daného zákazníka eGC

- jako samostatné SaaS služby, poskytující funkcionalitu celého IS nebo jeho podstatné části,
- jako jednotlivé IaaS a PaaS služby eGC v rámci čtyřvrstvé architektury IS – viz obrázek.



Obecné architektonické standardy dekompozice čtyřvrstvé architektury ISVS připravuje OHA v Informační koncepci ČR a souvisejících materiálech.

ŘOeGC bude připravovat a publikovat architektonické vzory využití služeb eGC v rámci IS.

5.1.5 Migrace IS do eGC

Projekt *Příprava vybudování eGC* nabízí a zpracovává dva pohledy na služby eGC a pravidla jejich použití.

Pohled využití služeb eGC v kontextu jednoho IS

Z tohoto pohledu poskytuje eGC nabídku standardizovaných služeb KeGC nebo SeGC, stanovuje jejich bezpečnostní a provozní standardy a definuje procesy usnadňující jejich využití.

Celkový koncepční pohled na proces migrace IS do eGC

Dlouhodobým koncepčním cílem eGC je využití služeb eGC pro migraci významné části IS v ČR na sdílené platformy a do datových center provozovatelů SeGC a KeGC, s cílem zajištění vyšší nákladové efektivity a bezpečnosti provozu těchto IS. Jde o dlouhodobý postupný proces.

V rámci budování eGC bude jednou z úloh ŘOeGC sledování, koordinace a plánování tohoto dlouhodobého procesu. Nástrojem pro řízení procesu migrace IS do eGC je katalog aktuálně provozovaných IS.

Pohled zákazníka eGC na proces migrace všech jeho IS do eGC

Lokální obdobou procesu migrace IS všech zákazníků eGC do eGC je pohled jednoho zákazníka eGC na migraci všech jeho IS do eGC. Migrace systémů jednoho zákazníka eGC do

eGC zajistí vyšší bezpečnost, vyšší kvalitu a nižší náklady provozu, umožní uvolnění stávajících datových center (po ukončení jejich životnosti), uvolnění kapacit IT pracovníků a jejich přesun z oblastí komoditních činností do oblastí řízení IT architektury a služeb.

Dočasným efektem migrace IS daného zákazníka eGC do eGC mohou být zvýšené náklady po dobu umístění části systémů v eGC a části ve vlastních datových centrech při nemožnosti dynamicky zmenšovat/snižovat vlastní kapacity.

5.2 Hodnocení úrovně bezpečnostních dopadů

Hodnocení závažnosti dopadů narušení bezpečnosti IS je v rámci eGC základním mechanismem kategorizace bezpečnostních požadavků IS (viz definice „**úroveň bezpečnostních dopadů IS**“ nebo „úroveň dopadů IS“). Možné dopady narušení bezpečnosti IS jsou následně mapovány na vhodnou úroveň bezpečnostních opatření služeb eGC, použitých pro implementaci a provoz IS (dále jen „**bezpečnostní úroveň služeb eGC**“). Stanovení požadované bezpečnostní úrovně služeb eGC je základním východiskem při umístění IS nebo jeho funkční části do komerční nebo státní části eGC. Úrovně bezpečnostních dopadů IS i bezpečnostní úrovně služeb eGC se určují na stupnici **1-4 (Nízká, Střední, Vysoká, Kritická)**.

5.2.1 Určení úrovně bezpečnostních dopadů IS

Metodika určení úrovně bezpečnostních dopadů IS a její mapování na požadovanou bezpečnostní úroveň služeb eGC je shrnuta v této kapitole a detailně popsána v příloze č. 4 *Metodika stanovení požadavků na bezpečnost IS*. Požadovaná bezpečnostní a provozní opatření, která musí implementovat provozovatel služeb eGC podle bezpečnostní úrovně poskytovaných služeb, jsou popsána v kapitole 6.

Úroveň závažnosti bezpečnostních dopadů IS je hodnocena z pohledu narušení důvěrnosti, integrity a dostupnosti, a případně totální ztráty dat. Pro hodnocení vybíráme ty oblasti dopadů, které vyjadřují hlavní funkce státu, důvěryhodnost jeho institucí, bezpečnost a svobody jeho obyvatel, až po finanční dopady obnovení normálního stavu. Zde použitá metodika navazuje na metodiku NÚKIB, publikovanou pod názvem „Metodika k vodítkům pro hodnocení dopadů“ (v1.2 z března 2018 - *https://www.govcert.cz/download/kii-vis/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf*). Tato metodika obsahuje 10 oblastí, odvozených od hodnocení dopadů kritické infrastruktury státu:

- bezpečnost a zdraví osob,
- ochrana osobních údajů,
- zákonné a smluvní povinnosti,
- trestně-právní řízení,
- veřejný pořádek,
- mezinárodní vztahy,
- řízení a provoz organizace,
- ztráta důvěryhodnosti,
- finanční ztráty,
- zajišťování nezbytných služeb.

Základem této metodiky (viz příloha č. 4) je tabulka „Vodítka pro určení závažnosti dopadů narušení bezpečnosti informací“, kde je uvedena stupnice závažnosti dopadů v úrovních 1 až 4 (Nízká, Střední, Vysoká, Kritická). Správci IS budou v **prvním kroku** určovat, jaké **maximální úrovně dopadu** mohou vůbec nastat při narušení důvěrnosti, integrity, dostupnosti jejich IS, až po ztrátu dat (od poslední zálohy, až po totální ztrátu dat). Tato metodika se bude primárně aplikovat na celý IS, avšak obdobným způsobem je možné ji aplikovat i na dekomponované části IS (například front-end prezentační vrstvu a back-end úložiště dat), resp. Na nižší

architektonické vrstvy (na aplikační vrstvu, na vrstvu platforem, a na vrstvu infrastruktury). Pravidla a příklady dekompozice IS pro tento účel budou rozpracována ŘOeGC a budou vycházet z pravidel dekompozice architektury IS určených OHA v návazných dokumentech na Informační koncepci ČR – po vrstvách architektury, podle služeb na jednotlivých vrstvách architektury, podle provozních prostředí apod.

5.2.2 Určení požadované bezpečnostní úrovně služeb eGC

V druhém kroku budou správci mapovat zjištěné maximální úrovně závažnosti dopadů převodní tabulkou na **požadované bezpečnostní úrovně služeb eGC**. Zjednodušeně řečeno:

- Úrovně dopadů 1 až 4 ve výše uvedených oblastech při narušení *důvěrnosti* a *integrity* se přímo aplikují na požadované bezpečnostní úrovně, se zohledněním pravidel pro hodnocení důležitosti aktiv ve 4 úrovních dle přílohy č. 1 vyhlášky č. 82/2018 Sb. (VoKB).
- Úrovně dopadů 1 až 4 se v oblasti narušení *dostupnosti* mapují na bezpečnostní úrovně hodnocením nárůstu dopadů s narůstajícím časem nedostupnosti. Správci zvažují rizika, zda deklarovaná dostupnost služeb eGC se započítáním podmínek SLA a statistik dostupnosti v určité bezpečnostní úrovni vyhovuje jejich časovým požadavkům na obnovení služby.

Metodika obsahuje i předepsané úrovně dostupnosti vyjádřené v %, společně s popisem způsobu měření (na měsíční bázi a případně se zohledněním definované pracovní doby).

Nabízené služby eGC (státní i komerční části) budou v katalogu služeb označeny svojí nejvyšší bezpečnostní úrovní 1 až 4, tedy úrovní, ve které splňují požadovaná kritéria zajištění důvěrnosti, integrity a dostupnosti. Z důvodu škálovatelnosti výkonu a cenové efektivnosti poskytování cloudové infrastruktury předpokládáme, že nabízené služby eGC budou muset současně splňovat požadavky dané úrovně 1 až 4 ve všech oblastech důvěrnosti, integrity a dostupnosti; přitom však lze akceptovat, že určité parametry SLA budou volitelné, tzn., že za účelem snížení ceny bude možné v rámci minitendru vyjednat slevu za snížení určitého parametru (zejména zajištění důvěrnosti versus dostupnosti), pokud to bude v dané architektuře cloudové služby možné a účelné. Z pohledu dodavatelů služeb eGC (státní i komerční části) panuje shoda v tom, že by nebylo praktické snažit se v katalogu eGC nabízet dané služby v příliš jemné granularitě oddělených aspektů úrovní důvěrnosti, integrity a dostupnosti, neboť úspory z rozsahu jsou dosahovány právě masívním využitím jedné cloudové infrastruktury, která musí být již od počátku navrhovaná pro dosažení určité bezpečnostní úrovně ve všech třech aspektech (důvěrnost, integrita, dostupnost).

Zařazení do úrovně dopadů a volba bezpečnostní úrovně je odpovědností správců IS, avšak v rámci zákazníků eGC bude třeba nastavit kontrolní mechanismy, zda výsledné zařazení do bezpečnostní úrovně není příliš nadhodnoceno nebo naopak podhodnoceno. Současně je důležité, aby počáteční hodnocení dopadů bylo prováděno v interakci mezi zkušeným bezpečnostním analytikem a správcem příslušného IS. První předběžné testy zařazování reálných IS jejich správci dle této metodiky také ukázaly, že je nutné jednotlivá posouzení úrovní dopadů a zařazení do bezpečnostních úrovní ověřit se správcem rozpočtu daného zákazníka eGC (náměstek ministra, ředitel úřadu).

5.2.3 Vztah k zákonům č. 181/2014 Sb. (ZoKB) a č. 412/2005 Sb. (Zákon o utajovaných informacích)

Vymezení metodiky úrovní dopadů a bezpečnostních úrovní vůči zákonu č. 181/2014 Sb. (ZoKB)

Pojem bezpečnostní úroveň „vysoká“ nebo "kritická" pro IS a služby eGC se přímo neváže na vymezení pojmů VIS, ISZS a KII dle §2 ZoKB, tzn. není zde přímé mapování bezpečnostních úrovní eGC na požadavky vyplývající ze ZoKB. Proces zařazení IS do bezpečnostních úrovní

funguje nezávisle na určovacím procesu KII a ISZS, avšak v maximální míře využívá již publikovaných vodítek NÚKIB pro hodnocení dopadů (viz úvod kapitoly 5.2.1 a příloha č. 4), a také vodítek pro hodnocení zpracovávaných aktiv dle vyhlášky č. 82/2018 Sb. (VoKB).

Tabulka úrovní dopadů uvedená v příloze č. 4 byla převzata z Metodiky k vodítkům pro hodnocení dopadů NÚKIB, publikované na https://www.nukib.cz/cs/kyberneticky-zakon/podpurne-materialy, viz dokument „Vodítka pro hodnocení dopadů – metodický materiál".

V případě, že je v některé z oblastí hodnocení dopadů narušení bezpečnosti (důvěrnost, integrita, dostupnost, ztráta dat) dosaženo úrovně dopadu 3 (Vysoká), popř. 4 (Kritická) může správce zvážit zařazení informačního systému mezi významné informační systémy (VIS).

Průřezová kritéria pro určení prvku kritické infrastruktury dle §1 nařízení vlády č. 432/2010 Sb. by měla odpovídat hodnocení dopadů IS nebo jeho dekomponované části v úrovni Kritická dle této metodiky.

Požadavky na bezpečnostní opatření v jednotlivých bezpečnostních úrovních byly v maximální možné míře odvozovány od stávajících požadavků, uvedených ve vyhlášky č. 82/2018 Sb. (VoKB). Aktuálně připravovaná nová vyhláška NÚKIB podle §6 (e) novely ZoKB, která definuje obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu (tzv. „cloudová vyhláška NÚKIB"), vzniká v koordinaci s projektem Příprava vybudování eGC na základě metodiky uvedené v tomto dokumentu.

Vymezení metodiky úrovní dopadů a bezpečnostních úrovní vůči zákonu č. 412/2005 Sb. (Zákon o utajovaných informacích)

Metodika a vodítka hodnocení nejsou určená pro informační systémy nakládající s utajovanými informacemi dle zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti. Na sdílené infrastruktuře eGC (včetně státní části eGC) není reálné splnění požadavků prováděcích předpisů k zák. č. 412/2005 Sb. a tím i zpracování utajovaných informací dle tohoto zákona.

5.2.4 Zpracování osobních údajů a vazba na Obecné nařízení GDPR

V bezpečnostní úrovni „nízká" (1) nelze zpracovávat osobní údaje.

V bezpečnostní úrovni „střední" (2) lze zpracovávat pouze osobní údaje s nízkým rizikem pro práva a svobody fyzických osob, které nespadají pod článek 35 GDPR.

Zpracování údajů, které dle čl. 35 GDPR bude mít pravděpodobně za následek vysoké riziko pro práva a svobody fyzických osob, bude moci využívat služeb eGC pouze v bezpečnostních úrovních 3 (Vysoká) a 4 (Kritická) podle výsledku „posouzení vlivu na ochranu osobních údajů" (DPIA). Povinné osoby posoudí rizika dle metodických pokynů ÚOOÚ a zvolí takovou bezpečnostní úroveň eGC služby (Vysoká nebo Kritická), která jim umožní zmírnění výchozích rizik zpracování pomocí dostupných bezpečnostních opatření na akceptovatelnou úroveň (což je zpravidla úroveň zbytkového rizika nízká nebo střední, dle použité metodiky hodnocení rizik). Viz GDPR Článek 35, odst. 7 d):

„plánovaná opatření k řešení těchto rizik, včetně záruk, bezpečnostních opatření a mechanismů k zajištění ochrany osobních údajů a k doložení souladu s tímto nařízením, s přihlédnutím k právům a oprávněným zájmům subjektů údajů a dalších dotčených osob"

Zpracování prováděná na základě zákonného zmocnění mají, dle současných legislativních pravidel, provedeno pouze posouzení dopadů na soukromí osob (PIA), a může být proto nutné doplnit rozsah těchto posouzení na formát DPIA dle čl. 35 GDPR a zapracovat požadavky na adekvátní opatření. Konkrétní úpravu povinnosti zpracovat posouzení vlivu DPIA pro orgány veřejné moci pravděpodobně přinese připravovaný „adaptační zákon".

Metodické pokyny ke zpracování DPIA jsou průběžně aktualizovány na webu ÚOOÚ, viz publikovaná vodítka Pracovní skupiny WP29 https://www.uoou.cz/pokyny-pracovni-skupiny-wp29/ds-4728/p1=4728, zejména dokument „Pokyny k posouzení vlivu na ochranu osobních

údajů a ke stanovení, zda zpracování bude „pravděpodobně mít za následek vysoké riziko“ pro účely Nařízení 2016/679“.

5.3 Kalkulace TCO

Hodnocení ekonomické výhodnosti je doplňujícím nástrojem pro celkové posouzení implementace a provozu IS v režimu on-premise (na vlastní infrastruktuře) nebo s využitím služeb eGC.

Metodika TCO (tj. Určení celkových investičních a provozních nákladů IS za 5 let provozu) je nástrojem eGC, který podporuje činnost správce IS, aby se mohl chovat jako správný hospodář. Metodika umožňuje porovnat celkové náklady různých variant provozu IS (zejména varianty eGC a varianty in-house provozu). Její plné nasazení se předpokládá zejména ve III. Fázi budování eGC - viz kapitola 10.

Metodika hodnocení ekonomické výhodnosti je shrnuta v této kapitole a detailně popsána v příloze č. 3 *Metodika určení TCO pro pořízení a provoz ICT služeb v rámci eGC*. Navazuje na Metodiku výpočtu TCO ICT služeb veřejné správy, vypracovanou Odborem hlavního architekta Ministerstva vnitra ČR (verze 3.61 z 15. 1. 2016). Metodiku TCO bude ŘOeGC dále rozvíjet a pravidelně aktualizovat.

Metodika kalkulace TCO umožňuje provést celou kalkulaci a srovnání buď v cenách bez DPH, nebo v cenách s DPH, podle charakteru vstupních finančních údajů zákazníka eGC. Obě srovnávané varianty musí být kalkulovány vždy stejným způsobem. Doporučený způsob kalkulace je včetně DPH, což je rovněž v souladu s běžně používanými metodikami ve státní správě.

Metodiku TCO využívá správce IS k prověření ekonomické výhodnosti migrace IS do eGC. Při posuzování TCO budou zohledňovány i možné zdroje financování, včetně dotací.

Kalkulace TCO je konečným výstupem ekonomického posouzení ICT služby, přičemž metodika řeší i kroky vedoucí k tomuto výstupu, především:

- přehledné **vymezení (definice) všech relevantních nákladů**, které jsou uplatňovány jak při pořízení, tak při provozu ICT služeb v režimu on-premise,
- **popis nákladových položek**, který bude plnit roli návodu a umožní správci IS určit hodnoty jako vstupy do kalkulace ekonomické výhodnosti,
- **stanovení hodnot** pro ty nákladové položky, které lze obecně uplatnit pro každou kalkulaci ICT služby napříč potřebami všech IS. Tyto údaje mají doporučující charakter a vycházejí z příkladů dobré praxe, zkušeností některých správců IS s kalkulací nákladů ICT služeb v předešlých letech, nebo legislativního vymezení,
- **porovnání ekonomické výhodnosti** ICT služby v režimu **on-premise** s pořízením ICT služby v **prostředí eGC**, a to na všech požadovaných úrovních (SaaS, PaaS, IaaS – podle povahy ICT služby),

Určení celkové ekonomické hodnoty požadované ICT služby po porovnání ekonomické výhodnosti ICT služby v režimu on-premise s pořízením ICT služby v prostředí eGC bude podkladem pro výběrové řízení a následné soutěžení ICT služby.

Vazba na bezpečnostní úrovně služeb eGC

Kalkulace TCO služby v režimu on-premise musí vzít v úvahu náklady na případné uvedení on-premise prostředí do souladu s požadavky bezpečnostní úrovně služeb eGC určené pro daný IS (bezpečnostní opatření odpovídající bezpečnostním standardům a opatřením uvedeným v kapitole 6). Poznámka: Požadavek na zajištění bezpečnostních opatření i pro on-premise provozované IS je pro ústřední správní úřady v souladu mj. s usnesením vlády č. 241/2018 z 18.4.2018.

Investiční a provozní financování IS

S využitím služeb eGC dojde z pohledu správce IS k postupnému přechodu od investičního financování (částí) IS k provoznímu financování. Sdílené služby eGC všech typů (od IaaS po SaaS) jsou z principu placené formou provozních poplatků a v ceně obsahují i rozpočítané investice provozovatele služeb. Tento princip je třeba reflektovat v plánování investičních a provozních rozpočtů v oblasti ICT.

Financování z fondů ESIF není vzhledem k provoznímu financování obecně aplikovatelné na nákup služeb eGC. *Poznámka:* Financování ESIF ale může být aplikovatelné na doprovodné aktivity jako jsou např. školení související s eGC a celou řadu aktivit v rámci vybudování SeGC (včetně např. Výstavby datových center). ŘOeGC bude monitorovat relevantní výzvy ESIF a koordinovat jejich využití.

5.4 Služby eGC

Příklady a ukázky služeb eGC a katalogů eGC uvedené v této kapitole nemají normativní, ale ilustrativní charakter. Rozpracování a další rozvíjení popsaných principů je úlohou ŘOeGC.

5.4.1 Přehled technických konceptů cloudových služeb

Tato kapitola shrnuje obecné technické koncepty a běžně používané termíny cloudových služeb (cloud computingu). Tyto koncepty jsou používány provozovateli eGC pro implementaci prostředí a služeb eGC. Terminologie služeb eGC vychází z terminologie obecných cloudových služeb. Ne všechny zmíněné koncepty jsou ale dostupné jako veřejná součást služeb eGC, přinejmenším v prvních fázích budování eGC. Na rozdíl od obecných cloudových služeb jsou v tomto dokumentu pod pojmem „služby eGC“ rozuměny výhradně ve smyslu, jak jsou a budou definovány v katalogu služeb eGC.

Virtualizace a cloudové služby

Pojmy virtualizace a pojem cloudové služby spolu těsně souvisí, avšak bývají často nesprávně zaměňovány

Virtualizací se rozumí vytvoření abstrakční vrstvy nad fyzickým HW serverů, která umožňuje spuštění více logicky oddělených virtuálních serverů, které se jejich uživatelům jeví jako skutečné servery. Tyto virtuální servery mohou mít různé operační systémy i připojený hardware. Obdobným principem lze virtualizovat i jiné typy HW zdrojů jako disková úložiště nebo komunikační sítě. Důležitou vlastností virtualizovaných zdrojů je skutečnost, že jsou vzájemně logicky odděleny a jeden uživatel tak nemůže přistupovat ke zdrojům jiného uživatele.

Cloudové služby (cloud computing) zahrnují nad rámec virtualizace řadu funkcí v oblasti správy a poskytování služeb:

- **Samoobslužné**: Uživatel může samostatně konfigurovat rozsah nakupovaných služeb jako např. Výkon virtuálních serverů nebo velikost datového úložiště.
- **Vysokorychlostní přístup přes síť**: Služby mohou být fyzicky umístěné kdekoliv.
- **Sdílené zdroje** pro **více uživatelů**: Uživatelé sdílejí stejné zdroje, ale jsou navzájem logicky izolováni, tj. nemohou zneužívat data a funkcionality jiných uživatelů.
- **Flexibilita, dynamičnost a škálovatelnost**: HW zdroje jsou přidělovány automaticky buď na požádání, nebo podle aktuální potřeby, z pohledu uživatelů se jeví neomezené.
- **Měření služeb**: Automatická kontrola a optimalizace zdrojů, platby podle skutečného využití zdrojů.

Orchestrací cloudových služeb je rozuměn (typicky automatizovaný a dynamický) proces konfigurace cloudových služeb. Orchestrační nástroje často podporují celou řadu různých

technologií a umožňují transparentně definovat abstraktní cloudové služby nezávislé na konkrétním typu HW.

Modely nasazení cloudových služeb

Privátní cloud je model nasazení virtualizace a dalších nástrojů cloudových služeb tzv. „on premise“ (ve vlastních prostorech) jediné organizace a jsou spravovány vlastními pracovníky organizace. Technologie cloudových služeb jsou využívány pro dynamickou orchestraci a sdílení mezi více organizačními složkami organizace nebo jednotlivými informačními systémy.

Veřejný cloud je model nasazení cloudových služeb tak, jak je dnes nejčastěji chápán – tedy jako poskytování cloudových služeb prostřednictvím Internetu třetí stranou, přičemž je zajištěna vysoká škálovatelnost a účtování podle využívaných zdrojů. Služby veřejného cloudu jsou typicky realizovány na velkých sdílených platformách pro mnoho zákazníků, v prostředí s vysoce pokročilou orchestrací a managementem, vysokým stupněm spolehlivosti, bezpečnosti
a škálovatelnosti a řadou dalších služeb.

Hybridní cloud: Koncept propojení cloudů, např. privátního cloudu a jednoho nebo několika veřejných cloudů, za účelem dynamického rozšiřování kapacit nebo zvýšení ekonomiky provozu při zachování bezpečnosti (části aplikací jsou umístěné v různých částech hybridního cloudu, podle jejich bezpečnostních požadavků). Orchestrační nástroje hybridního cloudu zajišťují jednotnou orchestraci cloudových služeb v celém prostředí.

Poznámka: Pojem Hybridní eGC souvisí jen částečně s obecným technickým pojmem „hybridní cloud“, jde o specifické uplatnění scénáře hybridního cloudu, kdy jsou služby provozovatele SeGC integrovány se službami provozovatelů KeGC. Nejde o scénář, kdy je on-premise cloudové prostředí zákazníka integrováno se službami eGC.

Cloud Broker

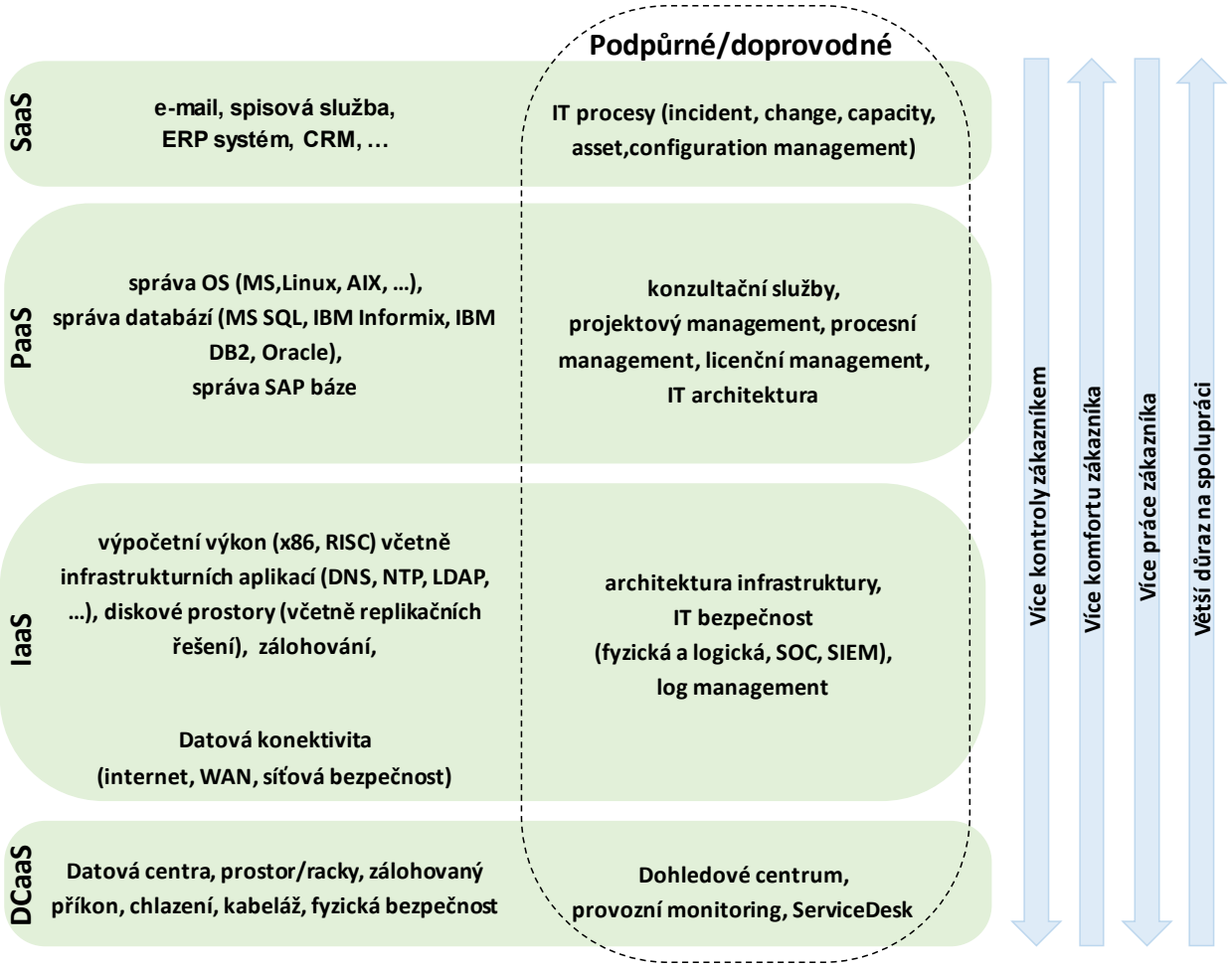
Cloud Broker je pokročilou službou pro jednotnou správu cloudových služeb v prostředí více provozovatelů veřejného cloudu. Může být provozován jako SW nástroj interně v jedné organizaci, může být poskytován dodavatelem veřejných cloudových služeb nebo jako samostatná veřejná služba. Cloud Broker obecně umožňuje:

- výběr cloudových služeb z nabídky více dodavatelů a jejich vzájemné porovnání (technických, smluvních i cenových parametrů),
- jednotný způsob nákupu vybraných služeb,
- jednotnou orchestraci služeb více dodavatelů,
- jednotný reporting služeb více dodavatelů.

Typy cloudových služeb - IaaS, PaaS, SaaS

Jednotlivé typy cloudových služeb se liší zejména administrativní hranicí, kde se dělí odpovědnost za provoz a rozvoj jednotlivých částí infrastruktury a aplikačního software mezi uživatelem a poskytovatelem cloudových služeb.

Následující obrázek ilustruje rozdělení jednotlivých vrstev infrastruktury podle typů cloudových služeb.



IaaS (Infrastructure as a Service - infrastruktura jako služba). Poskytování výpočetního výkonu, typicky virtuálního stroje s odpovídajícím úložným prostorem a síťovou konektivitou. IaaS služby lze vnímat jako pronájem virtuálních HW zdrojů. Uživatel se nemusí starat o dodávku, údržbu a provoz HW, jeho odpovědností je dodávka a správa SW od operačního systému výše.

Typickou IaaS službou je provoz virtuálního serveru dané CPU architektury (např. x86-64 nebo RISC) v požadované konfiguraci (počet core, velikost RAM) s připojením do komunikačních sítí. Jinou typickou IaaS službou je zajištění kapacity diskového prostoru o určitém objemu GB a výkonnostních parametrech IOPS.

Samostatnou součástí IaaS služeb na nejnižší úrovni jsou služby **housingu** (pronájmu prostoru v datovém centru spolu s odběrem elektřiny a síťovou konektivitou) pro umístění vlastního HW. Někdy hovoříme též o službách typu DCaaS (Data Center as a Service).

PaaS (Platform as a Service - platforma jako služba). Poskytování výpočetní infrastruktury spolu se standardními SW platformami jako jsou operační systémy, databáze, webové a aplikační servery. Uživatel se nemusí starat o dodávku a provoz HW a SW standardních platforem, pouze o aplikační SW.

Typickými PaaS službami jsou provoz virtuálního serveru včetně OS, provoz databází (např. MS SQL, Oracle, MySQL), provoz webových a aplikačních serverů (např. MS IIS, Apache, JBoss).

SaaS (Software as a Service - software jako služba). Poskytování kompletní aplikační funkcionality jako služby dostupné po síti. Uživatel se nemusí starat o implementaci ani aplikační správu aplikace, pouze definuje požadavky na její konfiguraci a integraci s jinými aplikacemi.

Typickými příklady SaaS služeb jsou e-mail, spisová služba, ERP systém, CRM apod. Nepovinnou součástí SaaS služeb jsou typicky i podpůrné aplikační služby potřebné pro provoz aplikací, jako Active Directory apod.

Hierarchie služeb. Součástí služeb jednotlivých typů jsou vždy služby všech nižších typů, tj. součástí služeb PaaS jsou vždy služby IaaS včetně housingu, součástí služeb SaaS jsou vždy služby PaaS. Služby nižších typů mohou být pro uživatele neviditelnou součástí služeb (např. U e-mailu platí za počet mailboxů, ne za výpočetní výkon HW na kterém mail server běží) nebo viditelnou součástí služeb (např. U e-mailu platí za objem uložených dat v mailboxech).

Podpůrné a doprovodné služby. Součástí všech typů služeb je typicky sada podpůrných provozních služeb, jako je provozní a bezpečnostní dohled, ServiceDesk pro evidenci a řešení incidentů a problémů služby. Nepovinné doprovodné služby jako správa licencí, podpora uživatelů, konzultační služby v oblasti IT architektury, aplikační analýzy a systémové integrace usnadňují uživateli při implementaci a využití cloudových služeb a správě jeho vlastního IT prostředí s využitím cloudových služeb.

5.4.2 Katalog služeb eGC

Katalog služeb eGC je seznam služeb eGC, který definuje služby eGC, jejich strukturu a hierarchii a jejich parametry.

Katalogový list služby eGC je popis jedné služby, určuje zejména parametry, kterými je daná služba definována.

Vzhledem k použitým soutěžním a nákupním mechanismům KeGC a SeGC je katalog služeb eGC ve skutečnosti tvořen sadou souvisejících katalogů:

- **Rámcový katalog služeb eGC** – v soutěžním mechanismu KeGC má roli předmětu zadání (poptávky po službách komerčních dodavatelů), popisuje strukturu a hierarchii služeb eGC, jejich povinné parametry a minimální smluvní podmínky a další související informace. Slouží zároveň jako primární společná struktura služeb pro všechny ostatní katalogy KeGC i SeGC. Je vytvořen a udržován ŘOeGC.
- **Katalog tržní nabídky služeb KeGC** obsahuje informace o službách dodavatelů, kteří se kvalifikují v daném soutěžním rámci, a to včetně detailních parametrů služby a indikativních cen. Strukturu katalogu a strukturu parametrů služeb určuje ŘOeGC, jeho obsah naplňují potenciální dodavatelé KeGC.
- **Katalog poptávek služeb KeGC** obsahuje konkrétní zadání minitendru soutěžního mechanismu KeGC. Jednotlivá zadání jsou tvořena zákazníky eGC v rámci minitendrů soutěžního mechanismu KeGC.
- **Katalog závazných nabídek služeb KeGC** obsahuje závazné nabídky dodavatelů KeGC včetně cen, které jsou odpovědí na poptávky služeb eGC v jednotlivých minitendrech soutěžního mechanismu KeGC. Vítězné nabídky (aktivní služby) jsou označeny a je k nim připojena smlouva.
- **Katalog služeb SeGC** obsahuje seznam a popis detailně definovaných, přímo objednatelných služeb eGC, vytvořený provozovateli SeGC ve spolupráci a pod kontrolou ŘOeGC.

Nabídka služeb v konkurenčním prostředí mnoha potenciálních dodavatelů KeGC je velmi variabilní (nabízí řadu variant služeb a řadu doprovodných služeb) a dynamická (rychle se mění v reakci na potřeby trhu a nabídky ostatních dodavatelů, často jsou zaváděny nové inovativní služby). Na rozdíl od SeGC nelze možnosti KeGC efektivně svázat do jednoho standardizovaného detailního katalogu služeb, a proto byl zvolen systém více katalogů, které zachycují nabídku trhu a reálné uzavřené smlouvy - viz kapitola 7.

Vytvoření a údržbu Rámcového katalogu služeb eGC a Katalogu služeb SeGC řídí ŘOeGC na základě požadavků zákazníků eGC a možností provozovatelů SeGC a KeGC. Katalogy služeb budou pravidelně aktualizovány, a to

- Rámcový katalog služeb eGC v souladu s časováním soutěžních rámců KeGC,
- Katalog služeb SeGC minimálně jednou za rok.

Rámcový katalog služeb eGC

Rámcový katalog služeb eGC určuje primární společnou strukturu služeb eGC pro všechny ostatní katalogy KeGC i SeGC. Rámcový katalog je vytvářen v časových verzích. Struktura katalogu může být v těchto verzích odlišná. Důvody změn struktury jsou: průběžná reakce ŘOeGC na změny v poptávce zákazníků eGC po službách eGC, změny v na IT trhu a získané zkušenosti ŘOeGC z využívání minulých verzí katalogu.

Následující sekce popisují prvotní návrh a příklad celkové struktury Rámcového katalogu služeb eGC. Tabulka obsahuje:

- definice typů služeb eGC: Typy služeb eGC (DCaaS, IaaS, PaaS, SaaS, podpůrné a doprovodné služby) jsou v katalogu služeb eGC definovány výčtem služeb,
- hierarchie služeb eGC: Služby v pravém sloupci jsou vždy podřízené službám v levém sloupci, tj. jsou jejich součástí,
- kvalifikační parametry: u každé služby jsou uvedeny požadované hodnoty základních kvalifikačních parametrů.

Legenda popisu: hierarchie služeb:

Přímo objednatelné služby	služby přímo objednatelné zákazníky eGC
Podřízené služby	služby objednatelné jako součást jiných služeb
Přímo objednatelné nebo podřízené služby	služby objednatelné přímo i jako součást jiných služeb

Podpůrné služby mohou být pro zákazníka eGC neviditelnou součástí služeb (např. U e-mailu platí za počet mailboxů, ne za výpočetní výkon HW na kterém mail server běží) nebo viditelnou součástí služeb (např. U e-mailu platí za objem uložených dat v mailboxech).

Služby eGC jsou zde uvedené na obecné úrovni, jejich konkrétní varianty vznikají určením vybraných technologických parametrů (např. architektura procesoru, typ operačního systému, …).

Hierarchie služeb DCaaS

Housing	Jednotka: Rack 800x1200 AND Rack 600x1200 Jednotka: kWh/měsíc Varianta: včetně/bez racku	→	Správa LAN	Jednotka: port 100Mbps OR 1Gbps OR 10Gbps
			Správa DWDM	Jednotka: Lambda
			Připojení Internet	Jednoka: Mbps Objem: minimálně 100Mbps
			Připojení CMS	Jednoka: Mbps Objem: minimálně 100Mbps
			Firewall	Jednotka: virtual FW instance
			Load-balancer	Jednotka: virtual LB instance
			VPN gateway	Jednotka: concurrent user

Služby housingu mohou být v eGC samostatně použity pouze za omezených podmínek – primárně jako dočasné služby v rámci urychlení migrace stávajících IS při zachování stávajícího HW. Zákazníci eGC nesmí investovat do nového HW, v případě obnovy HW musí přejít na vyšší služby IaaS nebo PaaS.

Hierarchie služeb IaaS

Diskový prostor	Technologie: Block Storage OR File Storage OR Mass Storage or Object Storage	→	Housing	
Výpočetní výkon	Technologie: x86 OR RISC (EBDIC) Technologie: Windows OR Linux OR Unix Varianta: bez OS OR Managed OS OR Unmanaged OS Jednotka: stavební blok vCPU + vRAM	→	Housing	
			Diskový prostor	
			Licence SW OS	
			IAM+PIM (jen pro Managed OS)	Jednotka: spravovaný účet
			Zálohování	Technologie: Místní OR Vzdálená záloha

Hierarchie služeb PaaS

Databáze	Technologie: Oracle OR DB2 OR Informix OR MS SQL OR MySQL OR PostgresSQL Technologie: standalone AND cluster Varianta: Managed and Unmanaged	→	Výpočetní výkon	
			Licence SW DB	Jednotka: ??? Účtování: PAYC
Aplikační servery	Technologie: IIS OR Apache OR J2EE Varianta: Managed and Unmanaged	→	Výpočetní výkon	
			Licence SW aplikačních serverů	Dle licenčního modelu SW
			Aplikační load balancing	

Hierarchie služeb SaaS

E-mail	Jednotka: Mailbox	→	Výpočetní výkon	
Spisová služba			Databáze	
HR systém			Aplikační servery	
Ekonomický systém				
Bezpečné uložiště dokumentů				
BI				

Podpůrné služby. Podpůrné služby jsou povinnou součástí všech typů služeb eGC.

			Provozní dohled	
			Bezpečnostní dohled (SIEM)	
			ServiceDesk	

Doprovodné služby. Doprovodné služby jsou nepovinným doplňkem služeb eGC. Rozdělení na komplexní služby a jednotlivé odborné role.

Správa licencí	
Podpora koncových uživatelů	
Konzultace - příprava minitendrů KeGC	Role: IT Architekt AND Bezpečnostní architekt AND Konzultant - právní Jednotka: MD
Systémová integrace - příprava a implementace	Role: IT Architekt AND Bezpečnostní architekt AND Analytik AND Projektový manažer Jednotka: MD
Systémová integrace - provoz	Role: IT Architekt AND Bezpečnostní architekt AND Analytik AND Projektový manažer AND Procesní manažer AND Bezpečnostní manažer Jednotka: MD

IT Architekt	Seniority: Junior AND Senior Jednotka: MD
Aplikační architekt	
Bezpečnostní architekt	
Procesní manažer	
Projektový manažer	
Bezpečnostní manažer	
Transition manažer	
Transformation manažer	
Architekt dohledových systémů	
DPO	Jednotka: MD

Speciální místo mezi doprovodnými službami mají **konzultační služby spojené s přípravou zadání minitendrů KeGC**. Zahrnují konzultace problematiky eGC, orientaci v katalozích služeb KeGC, posouzení prostředí a požadavků zákazníka včetně hodnocení bezpečnostních dopadů a kalkulací TCO, návrh technického řešení IS zákazníka s využitím služeb eGC a přípravu zadání minitendru KeGC.

Doprovodné a zejména konzultační služby nemá smysl rozdělovat podle bezpečnostních úrovní služeb eGC. Bylo proto určeno následující pravidlo pro využívání konzultačních služeb KeGC a SeGC: SeGC poskytuje konzultační služby pro služby SeGC (bezpečnostní úroveň 4) a hybridní eGC, KeGC poskytuje konzultační služby pro služby KeGC (bezpečnostní úroveň 1-3)

Katalogový list služby eGC

Katalogový list služby eGC obsahuje řadu parametrů. Struktura parametrů je určena ŘOeGC, jejich naplnění a význam závisí podle typu katalogu služeb eGC a podle typu služby. V soutěžním mechanismu KeGC budou mít některé parametry povinný (kvalifikační) charakter, tj. jejich splnění bude podmínkou přijetí nabídky dodavatele. Parametry služeb eGC mohou být naplněny požadovaným rozmezím nebo variantami hodnot (v případě poptávkových katalogů) nebo konkrétními hodnotami (v případě nabídkových katalogů).

Parametr katalogového listu „Bezpečnostní úroveň“ odpovídá požadavku, resp. závazku splnění architektonických, bezpečnostních a provozních standardů a opatření odpovídající bezpečnostní úrovně, uvedených v kapitole 6 (prvotní návrh, který bude dále rozvíjen a vyhlašován ŘOeGC). Vyplněná tabulka požadovaných opatření (včetně způsobu jejich naplnění) všech kvalifikovaných dodavatelů služeb KeGC bude publikována Portálu eGC.

Tabulka – Příklad katalogového listu služby eGC Výpočetní výkon a naplnění jeho parametrů v jednotlivých katalozích KeGC

Parametr	**Rámcový katalog** (soutěžní rámec) (X - povinný kvalifikační parametr)	**Katalog tržní nabídky** (příklad nabídky jednoho dodavatele - může obsahovat více variant služby)	**Katalog poptávek** (příklad zadání minitendru) (X - povinný parametr, H - hodnotící kritérium)	**Katalog závazných nabídek** (příklad odpovědi jednoho dodavatele v minitendru)
Základní parametry služby eGC				
Typ služby eGC	IaaS			
Bezpečnostní úroveň	1 OR 2 OR 3	3	3	3
Název služby eGC	Výpočetní výkon			
Zákazník			eGC zákazník 123	eGC zákazník 123
Provozovatel		eGC provozovatel 123		eGC provozovatel 123
Lokalita provozovatele	X EU	Kladno, Billund	X EU	Kladno
Místo poskytování služby		CMS OR NIX OR EU/Internet	X CMS	CMS
Popis služby (pokud možno rozdělený do co nejvíce pojmenovaných atributů, aby bylo snadné porovnávat)				
Soulad s legislativou a normami				
Základní funkce				
Volitelné funkce				
Podporovaná uživatelská rozhraní				
Jazyky uživatelského rozhraní				
Integrační rozhraní				
Administrativní rozhraní				
Technologické, objemové a cenové parametry služby Výpočetní výkon				
Technologie	X x86 OR RISC (EBDIC), bez OS	x86-64	X x86-64	x86-64
Technologie	X Windows OR Linux OR Unix	Windows (2013, 2016) OR Linux (RedHat, Centos)	X Windows 2016	Windows 2016
Varianta	X Bez OS AND Managed OS AND Unmanaged OS	Bez OS AND Managed OS AND Unmanaged OS	X Managed OS	Managed OS
Frekvence		3,2GHz OR 3,6GHz	X minimálně 3,2GHz	3,2GHz

Jednotka	X stavební blok vCPU+vRAM	stavební bloky vCPU+vRAM: 1vCPU+2GB vRAM OR 1vCPU+4GB vRAM OR 1vCPU+8GB vRAM	X poměr vCPU a vRAM – 1:4GB	poměr vCPU a vRAM – 1:4GB
Měření a účtování objemu služby		Fixed or PAYC	X PAYC	PAYC
Objem služby		min 2 vCPU	X min 10 vCPU, max 20 vCPU	min 20 vCPU, max 20 vCPU
Cena služby		1vCPU+2GB vRAM 1000 Kč/vCPU/měsíc 1vCPU+4GB vRAM 1100 Kč/vCPU/měsíc 1vCPU+8GB vRAM 1300 Kč/vCPU/měsíc	H max 1000 Kč/vCPU/měsíc	998 Kč/vCPU/měsíc
Technologické, objemové a cenové parametry podřízené služby Diskový prostor				
Součást služby	X Ano	Ano	X Ano	Ano
Technologie	X Block Storage OR File Storage OR Mass Storage OR Object Storage	Block Storage OR File Storage	X Block Storage	Block Storage
IOPS	specifikujte pro čtení i zápis	35000/10000 OR bez garancí	X 35000/10000	35000/10000
Propustnost	specifikujte v MB/s	2000MB/s OR bez garancí	X 2000MB/s	2000MB/s
Jednotka		GB	X GB	GB
Měření a účtování objemu služby		Fixed or PAYC	X PAYC	PAYC
Objem služby		min 100 GB	X min 10 GB, max 5000 GB	min 10 GB, max 5000 GB
Cena služby		IOPS 35000/10000, 2GB/s 5 Kč/GB/měsíc bez garancí 3 Kč/GB/měsíc	H max 4 Kč/GB/měsíc	3,95 Kč/GB/měsíc
Technologické, objemové a cenové parametry podřízené služby Zálohování				
Součást služby	X Ano	Ano	X Ano	Ano
Technologie	X Místní OR Vzdálená záloha	Místní OR Vzdálená záloha	X Místní záloha	Místní záloha
Jednotka		GB	X GB	GB
Měření a účtování objemu služby		Fixed OR v ceně služby Diskový prostor	X V ceně služby Diskový prostor	V ceně služby
Objem služby		min 100 GB		
Cena služby		Fixed: 2 Kč/GB/měsíc		
Technologické, objemové a cenové				

parametry podřízené služby IAM+PIM				
Součást služby	Ne	Ano	X Ne	Ne
…				
Technologické, objemové a cenové parametry podřízené služby Připojení CMS				
Součást služby	X Ano	Ano	X Ano	Ano
Jednotka	X Mbps	Mbps		
Měření a účtování objemu služby		Do 100Mbps v ceně OR Fixed limit in Gbps	Limit 100Mbps	Limit 100Mbps
Objem služby	X minimálně 100Mbps	100Mbps – 10Gbps	X max 100Mbps	max 100Mbps
Cena služby		Fixed: 10000 Kč/Gbps/měsíc	H	V ceně služby
Technologické, objemové a cenové parametry podřízené služby Připojení Internet				
Součást služby	X Ano	Ano	X Ne	Ne
…				
Technologické, objemové a cenové parametry podřízené služby Firewall				
Součást služby	X Ano	Ano	X Ano	Ano
…				
Technologické, objemové a cenové parametry podřízené služby Load-balancer				
Součást služby	X Ano	Ano	X Ne	Ne
…				
Technologické, objemové a cenové parametry podřízené služby VPN Gateway				
Součást služby	Ne	Ano	X Ne	Ne
…				
Kvalitativní parametry - příklady				
Provozní doba celková (provoz)	X 7x24	7x24	7X24	7X24
Provozní doba aktivní (podpora)	X dle požadavků dostupnosti dané 47bezpečnostní úrovně	BÚ 3 a 2: 7x24 BÚ 1: Pracovní dny 7:00-19:00	7X24	7X24
SLA dostupnosti	X dle požadavků dostupnosti dané 47bezpečnostní úrovně	99,90%	99,90%	99,90%
SLA řešení incidentů a provozních požadavků				
Testovací/školicí prostředí		Ano	X Ano	Ano
…				

Smluvní parametry – příklady				
Doba trvání služby	X minimálně 2 roky	maximálně 7 let	X 4 roky	4 roky
Podmínky výpovědi smlouvy	maximálně 6 měsíců	minimálně 3 měsíce	X 3 měsíce	3 měsíce
Podpora migrace služby k jinému dodavateli	X Ano	Ano		
SLA penále				
…				

Katalog služeb SeGC

Bude obsahovat seznam a popis detailně definovaných, přímo objednatelných služeb eGC, včetně cen, vytvořený provozovateli SeGC ve spolupráci a pod kontrolou ŘOeGC.

Struktura Katalogu služeb SeGC odpovídá sktruktuře Rámcového katalogu služeb eGC. V porovnání s katalogy služeb KeGC je Katalog služeb SeGC obdobou sady nabídek jednoho dodavatele v Katalogu tržní nabídky KeGC.

Katalog služeb SeGC bude pravidelně aktualizován, a to minimálně jednou za rok.

Katalog služeb bude dále průběžně doplňován o nové služby, vytvořené na základě individuálních požadavků jednotlivých zákazníků eGC, projednaných s provozovateli SeGC a ŘOeGC. V tomto případě nejde o budování vysokého množství velmi specifických služeb, každý takový požadavek zákazníků eGC bude zobecněn a vnímán jako podnět k vytvoření nové služby nebo rozšíření stávající obecně použitelné služby.

Popisy i ceny služeb uvedených v katalogu služeb SeGC jsou schvalovány ŘOeGC.

Hybridní eGC

V případě použití modelu hybridního eGC použije zákazník eGC pro výběr a objednání služeb katalog služeb SeGC. Cena části služeb, realizovaných pomocí KeGC, je upravena na základě reálné ceny použitých KeGC služeb.

5.4.3 Portál eGC

Portál eGC je nástroj pro ŘOeGC, provozovatele eGC a zejména pro správce IS. Jeho cílem je maximálně usnadnit využití a správu služeb eGC.

Portál eGC slouží k

- publikaci metodických, statistických a dalších informací ŘOeGC pro správce IS i pro provozovatele eGC,
- publikaci katalogů eGC,
- orientaci správců IS (zákazníků eGC) v katalozích eGC, výběr služeb eGC a sestavení podkladů pro zadání objednávek SeGC nebo minitendrů KeGC,
- integraci s elektronickými tržišti (NEN) a podpoře administrativního procesu zadávání minitendrů eGC,
- jednotnému integrovanému reportingu služeb eGC všech provozovatelů eGC.

Za funkcionalitu portálu odpovídá ŘOeGC.

Cílovou funkcí Portálu eGC je i přímé zadávání a objednávání služeb (funkce elektronického tržiště). Tato funkce ale vyžaduje legislativní změny.

Portál eGC bude postupně naplňovat funkce Cloud Brokeru. Musí být integrován s existujícími elektronickými tržišti, nebo se sám stát elektronickým tržištěm v souladu se ZZVZ.

V rámci pilotních projektů SeGC a KeGC proběhne i **pilotní projekt Portálu eGC**, který bude zahrnovat:

- studii proveditelnosti, výběr a otestování nástrojů, funkční specifikace,
- implementaci první verze Portálu eGC.

5.5 Nákup služeb eGC

Tato kapitola rozvíjí a popisuje ve větší míře detailu nákupní procesy SeGC a KeGC popsané v kapitolách 4.5 a 4.6.

Poznámka: *Tato kapitola (a ostatní kapitoly mimo kapitoly 7) využívá pro odkazy na soutěžní mechanismus KeGC obecnou terminologii (soutěžní rámec, kvalifikace, minitendr, zadání, poptávka, nabídka, …) bez přímé konkrétní vazby na terminologii a mechanismy ZZVZ. Cílem je popsat používané soutěžní mechanismy z procesního a praktického pohledu. Vazba na konkrétní mechanismy a terminologii ZZVZ je popsána v kapitole 7.*

5.5.1 Nákup služeb SeGC

Zákazník eGC nakupuje služby SeGC na základě výběru z katalogu SeGC, přímým kontraktem s provozovatelem SeGC, na základě výjimky ze ZZVZ. Tento postup předpokládá nákladovou definici cen služeb SeGC schválenou zakladateli a kontrolovanou ŘOeGC pro zajištění ekonomické efektivity využívání SeGC.

5.5.2 Soutěžní mechanismus KeGC

Právní a organizační rámec KeGC je navržen na základě osvědčených zkušeností s fungováním government cloudu ve Velké Británii a Dánsku a modifikován tak, aby respektoval ZZVZ.

Pro nákup služeb KeGC bude dvoustupňový soutěžní mechanismus (soutěžní rámce, minitendry) s centrálním zadáváním, který musí umožnit:

- průběžné přistupování nových zadavatelů (zákazníků eGC),
- průběžné přistupování (kvalifikace) nových dodavatelů.

Centrálním zadavatelem pro KeGC bude v souladu s kompetenčním zákonem Ministerstvo vnitra (ŘOeGC).

V rámci pilotního projektu KeGC a pilotního projektu Portálu eGC budou posouzeny a případně navrženy legislativní a procesní změny pro budoucí právní a organizační rámec KeGC.

5.5.3 Soutěžní rámce KeGC

V průběhu času se na základě vývoje technologií a standardů a na základě zkušeností s budováním a organizací KeGC budou vyvíjet také předmět (služby eGC) a kvalifikační požadavky (bezpečnostní a provozní standardy jednotlivých bezpečnostních úrovní atd.) soutěžního mechanismu KeGC. Opakovaně v čase budou vypisovány nové soutěžní rámce, vždy s aktualizovaným zadáním. Soutěžní rámce a platnost smluv uzavřených na jejich základě se mohou časově překrývat (aby byla zajištěna kontinuální možnost nákupu a čerpání služeb KeGC) – viz obrázek v kapitole 4.6.

Vzhledem k tomu, že vývoj struktury a popisu služeb bude pravděpodobně probíhat pro různé typy služeb eGC různým tempem (např. stabilnější IaaS versus dynamicky se rozvíjející SaaS služby), bude soutěžní mechanismus KeGC rozdělen do sady paralelních soutěžních rámců, odpovídajících částem katalogu služeb KeGC.

Strukturu soutěžních rámců KeGC a jejich časování určuje ŘOeGC. ŘOeGC bude zveřejňovat jednoznačný a konkrétní časový plán soutěžních rámců KeGC.

Časová platnost smluv uzavřených na základě soutěžního rámce není vázána na časovou platnost vlastního soutěžního rámce. Starý soutěžní rámec lze uzavřít nebo přestat vypisovat další minitendry, uzavřené smlouvy zůstávají v platnosti i po uzavření soutěžního rámce.

Zadání soutěžního rámce KeGC a kvalifikace dodavatelů

Zadávací dokumentace každého soutěžního rámce KeGC bude obsahovat:

- pravidla a vzorové dokumenty soutěžního rámce,

- rámcový katalog služeb eGC, resp. jeho část, která určuje předmět soutěžního rámce, včetně definice požadované dokumentace k prokázání souladu s povinnými parametry služeb (schopnost dodávat služby),
- seznam povinných bezpečnostní opatření pro jednotlivé bezpečnostní úrovně, včetně definice požadované dokumentace k jejich prokázání,
- další kvalifikační požadavky.

ŘOeGC navrhne, registruje a bude spravovat sadu NIPEZ (CPV) kódů vhodných pro služby eGC.

Před vypsáním každého soutěžního rámce ŘOeGC provede analýzu aktuálních potřeb veřejné správy (na základě informací v Katalogu aktuálně provozovaných IS), zohlední stav a vývoj technologických možností nových cloudových služeb a aktualizuje Rámcový katalog služeb eGC.

Některé parametry katalogových listů Rámcového katalogu služeb eGC budou označeny jako povinné (kvalifikační) a jejich splnění je předmětem hodnocení kvalifikace (schopnost uchazeče dodávat dané služby eGC).

Poté ŘOeGC ve spolupráci s OVZ MV vyhlásí soutěžní rámce pro jednotlivé skupiny služeb.

Vzhledem k vysoce odborné problematice hodnocení souladu uchazečů s povinnými parametry služeb a souladu s požadavky na bezpečnostní opatření musí být do hodnotící komise pro hodnocení kvalifikace dodavatelů dostatečný počet členů s odbornou kvalifikací v oblastech IT a bezpečnosti.

Části soutěžního rámce KeGC

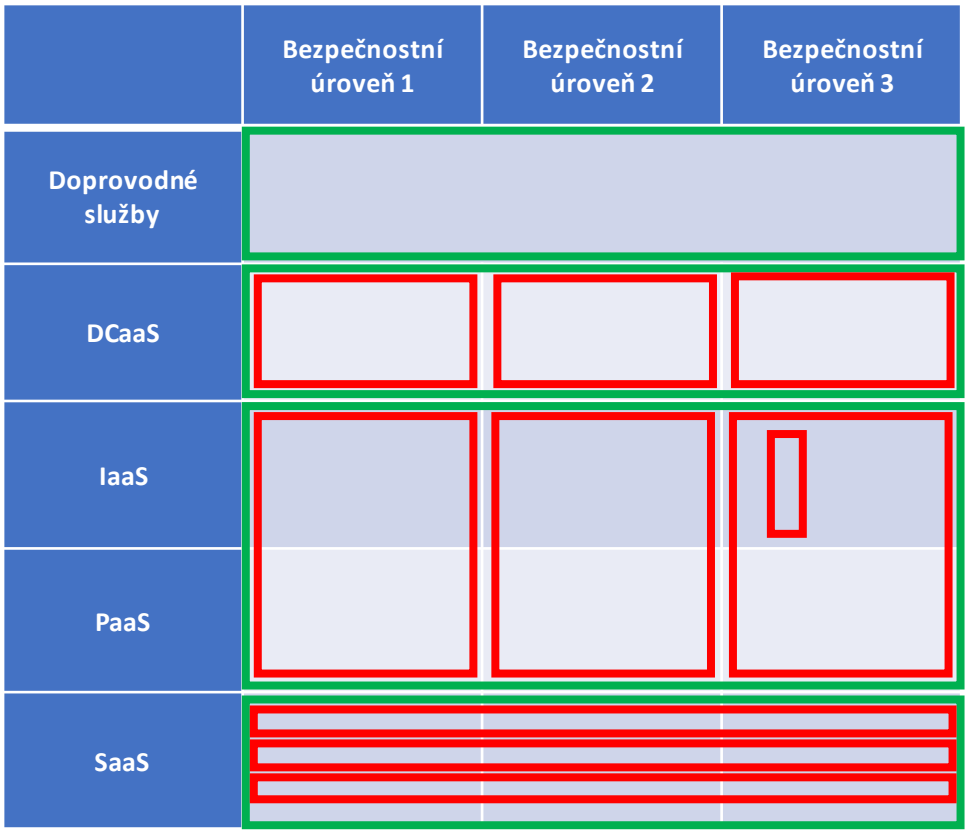
Každý soutěžní rámec KeGC může být rozdělen do sady samostatných částí s různými technickými kvalifikačními požadavky. Technické kvalifikační požadavky jednotlivých částí budou zahrnovat:

- splnění bezpečnostních a provozních požadavků příslušné bezpečnostní úrovně služeb eGC,
- schopnost poskytovat služby příslušné části katalogu v rozsahu povinných požadavků,

Kvalifikační požadavky pro každou část soutěžního mechanismu KeGC musí být formulovány tak, aby kvalifikaci mohlo splnit více dodavatelů. Jeden dodavatel se může kvalifikovat do jedné, více i všech částí. Zadavatel minitendru si pak vybírá část soutěžního rámce, ve které soutěží minitendr.

Cílem rozdělení soutěžních rámců na části je zjednodušení soutěže minitendru pro zákazníky eGC, který si může vybrat část nejlépe odpovídající typu minitendru a oslovit skupinu kvalifikovaných dodavatelů co nejlépe odpovídajících požadovaným službám a jejich parametrům. *Příklad: Pokud bychom soutěžní rámec KeGC nedělili, zákazník eGC požadující pouze službu výpočetního výkonu by v minitendru oslovoval i všechny dodavatele konzultačních služeb a všech typů PaaS a SaaS služeb.*

Z pohledu pokrytí Rámcového katalogu služeb eGC se jednotlivé soutěžní rámce i jejich části mohou navzájem překrývat. Rozdělení soutěžních rámců na části určuje ŘOeGC při jejich vypsání. Následující diagram znázorňuje ilustrativní příklady rozdělení Katalogu služeb KeGC na sadu soutěžních rámců a jejich částí. Zelené rámečky zobrazují soutěžní rámce, červené rámečky zobrazují jejich části.



Na obrázku jsou znázorněny čtyři soutěžní rámce vycházející z rámcového katalogu:

- soutěžní rámec na doprovodné služby – pro samostatné zakázky na konzultační služby,
- soutěžní rámec na DCaaS služby, rozdělený na tři části po bezpečnostních úrovních – pro samostatné zakázky na DCaaS služby,
- soutěžní rámec na IaaS a PaaS služby, rozdělený na tři části po bezpečnostních úrovních – pro kombinované zakázky typu „platforma pod komplexní IS“,
- soutěžní rámec na SaaS služby, rozdělený na části po jednotlivých oblastech služeb (spisová služba, ekonomické systémy, …) – pro samostatné zakázky na SaaS služby.

V soutěžním rámci na IaaS a PaaS služby je dále uveden příklad speciální zúžené části IaaS služeb na nejběžnějších HW platformách (např. x86) – pro samostatné zakázky na IaaS služby na konkrétní HW platformě.

Poznámka ke kombinovaným minitendrům: při nákupu kombinace více služeb v jednom minitendru (tj. Najednou od jednoho dodavatele) musí na straně zákazníka eGC existovat konkrétní důvod pro sdružení do jedné zakázky (technický, provozně ekonomický).

Poznámka k minitendrům na služby omezené na konkrétní HW/SW platformu: na straně zákazníka eGC musí existovat konkrétní důvod omezení soutěže na konkrétní variantu služby (např. technická kompatibilita, ochrana investic, …).

Katalog tržní nabídky služeb KeGC

Dodavatelé zveřejní informace o svých jednotlivých službách v Katalogu tržní nabídky KeGC a dále je mohou aktualizovat po celou dobu trvání soutěžního rámce. Nabídky služeb KeGC budou zadávány prostřednictvím Portálu eGC a musí být ve formátu katalogových listů Katalogu tržní nabídky KeGC.

Po uložení nabídky na Portál eGC ŘOeGC provede její posouzení, tj., zda dodavatel a jeho nabídka splňuje povinné (kvalifikační) podmínky daného soutěžního rámce.

Při kontrole ŘOeGC zejména posuzuje:

- zda nabízená služba je v souladu s předmětem soutěžního rámce (služby Rámcového katalogu),
- zda dodavatel prokázal naplnění bezpečnostních opatření požadovaných pro danou bezpečnostní úroveň,
- zda služba je v souladu s pravidly stanovenými OHA,
- zda ekonomické podmínky služby jsou v definovaných limitech.

Posouzení proběhne v definovaném čase od příchodu nabídky. Rozhodnutí o případném odmítnutí informace o službě dodavatele musí ŘOeGC odůvodnit.

Akceptované nabídky ŘOeGC zveřejní na Portálu eGC v Katalogu tržní nabídky služeb KeGC.

ŘOeGC umožní po celou dobu trvání soutěžního rámce dodavateli upravit informace o službách, a to za předpokladu, že zůstane nadále v souladu s požadavky soutěžního rámce.

5.5.4 Minitendry KeGC

Zadání minitendru KeGC obsahuje

- pravidla a vzorové dokumenty minitendru, včetně určení části soutěžního rámce KeGC, a časové platnosti smlouvy,
- seznam a objem požadovaných služeb eGC a jejich konkrétní požadované parametry
- smluvní podmínky (vzor smlouvy),
- hodnotící kritéria aplikovaná v minitendru.

Parametry katalogových listů zadání minitendru KeGC budou rozděleny na povinné a hodnotící. Hodnotícím parametrům je přiřazena jejich váha.

Zadání může určit maximální cenu minitendru (např. V souladu s kalkulací TCO provedenou zákazníkem eGC).

Zadání minitendru KeGC sestavuje správce IS (zákazník eGC) na základě

- znalosti svého prostředí a svých potřeb. Přípravnými kroky jsou hodnocení bezpečnostních dopadů IS, návrh architektury IS s využitím služeb eGC, případně kalkulace TCO, získání stanoviska OHA atd.,
- zadávací dokumentace soutěžního rámce KeGC (procesní pravidla soutěžního rámce, Rámcový katalog služeb eGC, část soutěžního rámce),
- katalogy služeb KeGC popisující reálnou nabídku trhu a zkušenosti z předchozích minitendrů – Katalog tržní nabídky služeb KeGC, Katalog poptávek služeb KeGC, Katalog závazných nabídek služeb KeGC.

Pro zjednodušení procesu přípravy zadání minitendrů může zákazník eGC využít

- metodiky a vzory publikované ŘOeGC,
- konzultační služby, samostatně objednané jako služba eGC,
- (do budoucna) pokročilé funkce Portálu eGC a jeho integraci s elektronickými tržišti.

Při nákupu kombinace více služeb v jednom minitendru musí existovat důvod pro sdružení do jedné zakázky (technický, provozně ekonomický).

Zadání jednotlivých minitendrů jsou uložena a zveřejněna v Katalogu poptávek služeb KeGC.

Nabídky do minitendru KeGC

Nabídky mohou podat dodavatelé kvalifikovaní pro danou část soutěžního rámce KeGC. Nabízené služby dodavatel popíše ve formě katalogových listů eGC. Dodavatel musí splnit

povinné parametry všech služeb požadovaných v minitendru. Hodnoty hodnotících parametrů v nabídce dodavatele zadavatel použije pro hodnocení nabídky.

Nabídky dodavatelů do jednotlivých minitendrů jsou uloženy a zveřejněny v Katalogu závazných nabídek služeb KeGC.

Hodnoty parametrů nabízených eGC služeb nemohou být horší než ty, které byly uvedeny v informacích o službách dodavatele do Katalogu tržní nabídky KeGC.

Hlavním hodnotícím kritériem minitendru KeGC je ekonomická výhodnost nabídky. Dílčí hodnotící kritéria musí být formulována v souladu se ZZVZ a mohou být stanovena na základě vztahu obsahových, objemových a kvalitativních charakteristik služby eGC a ceny:

- Hodnotící kritéria ceny – mohou být založena na celkové ceně minitendru (při stanovení fixního objemu služeb) nebo na kombinaci jednotkových cen služeb eGC (při použití principu pay-as-you-consume, viz níže).
- Hodnotící kritéria kvality – mohou být založena na plnění hodnotících parametrů služeb nebo plnění povinných parametrů nad rámec stanovených požadavků.

V případě, že zákazník eGC poptává integrační službu (kupříkladu včetně podpory a záruk za úspěšnou transformaci IS a integraci KeGC služby do IS) může být hodnotícím kritériem i kvalita nabízené integrační služby.

Dynamické čerpání služeb eGC – PAYC

Princip dynamického čerpání služeb (pay-as-you-consume, PAYC – měření služeb a platby podle jejich skutečného využití) je jeden ze základních principů cloudových služeb. V eGC lze tento princip využít pro několik účelů:

- automatizované dynamické čerpání (měřené po časových, výkonnostních a objemových jednotkách) pro systémy s nepravidelnými nároky na výkon nebo objem služby,
- manuálně konfigurované změny v čase – např. posílení platformy v termínu pravidelných ročních podání, změny počtu uživatelů aplikace,
- dlouhodobý rozvoj systému – např. rozšíření platformy o nová vývojová/testovací prostředí, doplnění nového modulu systému apod.

Ve všech těchto případech stanoví zákazník eGC v zadání minitendru celkovou dobu trvání smlouvy, seznam služeb eGC, pro každou z nich minimální a maximální limity čerpání a časovou granularitu měření objemu čerpaných služeb (minuta, hodina, den, měsíc, …). Nabídka dodavatelů KeGC pak musí obsahovat jednotkové ceny všech požadovaných služeb za určený časový úsek. Pro hodnocení ceny nabídky je pak třeba stanovit váhy jednotlivých služeb (spotřební koš).

Poznámka: Použití principu PAYC pro zajištění dlouhodobého rozvoje platformy u jednoho dodavatele KeGC je nutno odůvodnit technickými nebo provozně ekonomickými argumenty.

5.6 Výhody a rizika využívání eGC

5.6.1 Výhody a rizika podle typu služeb eGC

Výhody obecně (všechny typy služeb):

- Cenový model – pay-per-use/pay-as-you-consume (platí se jen za skutečně spotřebované zdroje).
- Technologické inovace – zákazník má v cloudových službách obvykle přístup k nejnovějším technologiím a zkušenostem na světové úrovni, protože cloudové služby jsou hlavním předmětem podnikání poskytovatele.

- Investice do rozvoje zajišťuje dodavatel služby – eliminace investičních nákladů do IT na straně zákazníka.
- Provoz a servis v režimu 24x7.
- Vysoká garance bezpečnosti, spolehlivosti a dostupnosti definovaná smlouvou.
- Krátká doba reakce na incidenty.
- Rychlá obnova dat po haváriích.
- Automatizace procesů služeb Cloud computingu.
- Poskytování monitorovacích nástrojů bez dodatečných nákladů.
- Možné škálování odebíraného objemu služeb v čase (nahoru i dolů).
- Žádné dodatečné poplatky za škálování.
- Malé a střední instituce mohou využívat stejně dokonalou technologii a funkcionalitu jako velcí.
- Možnost otestovat službu před jejím zakoupením.
- Schopnost snížit náklady na podnikání s úsporami IT nákladů. Nižší celkové náklady jsou umožněny multiplicitním využíváním týchž zdrojů více zákazníky najednou a jednodušším modelem dodávky služby. Náklady na ICT jsou pro zákazníka jasně viditelné a predikovatelné, jsou rovnoměrně rozloženy v čase, nejsou investiční povahy. Díky škálovatelnosti služeb výše nákladů může korelovat s objemem odebíraných služeb.

Motivace k migraci na služby eGC:

- Využití eGovernment technologií (JIP/KAAS, NIA, eGSB) a soulad s požadavky GDPR na straně zpracovatele bude součástí SaaS služeb eGC, přechodem na SaaS služby eGC je správce získá „zadarmo“.
- Rychlost implementace IS (nasazuji služby, které již existují).
- Cenová efektivnost – platím jen za to co spotřebuji, a proto si toho mohu dovolit koupit více z hlediska sortimentu.
- Některé eGC služby budou na vysoké úrovni bezpečnosti a odolnosti, a proto se budu moci pustit i do elektronizace služeb s vysokou úrovní dopadů, což bych dříve s omezenými prostředky nemohl.

Rizika obecně:

Následující seznam uvádí rizika, která platí pro všechny typy služeb. Vhodným způsobem řízením eGC a provozovatelů eGC je však možné je překonat.

- Výběr vhodného poskytovatele služby.
- Stabilita poskytovatele – nenadálé ukončení služby (Návratová strategie).
- Bezpečnost.
- Důvěryhodnost a soukromí dat.
- Lock-in na jednoho dodavatele.
- Legislativa.
- Odpor vlastního IT útvaru.

Výhody SaaS:

- SW licence se nekupují (užití licence je součástí ceny služby). Platí se pouze za služby, které byly v daném období objednány, resp. Využity.
- Architektura aplikace je navržena tak, aby tutéž aplikaci ve stejné době mohly využívat tisíce uživatelů z mnoha různých organizací (víceuživatelská aplikace, multi-tenantní architektura).

- Vysoká dostupnost služeb SaaS a dat díky masívní redundanci výpočetních zdrojů a uložení dat.
- Služba je relativně rychle využitelná díky krátkému implementačnímu cyklu. Obvykle nevyžaduje u zákazníka instalovat žádný nový HW ani SW.
- Nové verze SW mohou být uváděny do provozu často (2 – 4x ročně). Upgrade je realizován pouze provozovatelem. Všichni zákazníci obvykle využívají stejnou verzi a jsou převedeni na novou verzi dle předem ohlášeného plánu. To poskytovateli služby snižuje náklady provozu aplikace a současně urychluje vývojový cyklus aplikace.
- Aplikace může být (obvykle zdarma) vyzkoušena v testovacím provozu před zakoupením.
- Pouze velmi málo technologických a lidských zdrojů se na straně zákazníka používá pro ICT podporu.

Rizika SaaS:

- Úpravy aplikace a aktivace nových verzí mimo kontrolu zákazníka.
- Data jsou uložena mimo vlastní organizaci.
- Nižší možnosti customizace aplikace pro jednotlivé zákazníky.
- Nezajištěná integrace s ostatními aplikacemi.

Výhody IaaS a PaaS:

- Škálovatelnost odebíraných služeb.
- Podpora řady různých provozních platforem (zejména operačních systémů).
- Konfigurovatelné funkce (CPU, RAM, datový sklad).
- Nejnovější technologické hardwarové a softwarové prostředky.
- Nastavení geografické redundance výpočetních zdrojů dle volby zákazníka.

Rizika IaaS a PaaS:

- Data jsou uložena mimo vlastní organizaci.

5.6.2 Výhody využití soutěžního mechanismu KeGC

Společné katalogy služeb KeGC

- Analýza aktuálních potřeb potenciálních zákazníků eGC prováděné ŘOeGC, která vezme v úvahu aktuální potřeby, architekturu a rozvojové plány zákazníků eGC, zajistí pokrytí potřeb zákazníků eGC a zároveň směrování ke standardizaci využívaných služeb. Zároveň budou vždy zajištěny společné bezpečnostní a provozní standardy.
- Katalog tržní nabídky KeGC a Katalog závazných nabídek KeGC umožní správcům IS rychlou, aktuální a transparentní orientaci na trhu provozovatelů služeb KeGC.
- Při zadání minitendru může správce IS určit doplňující podmínky služeb podle svých specifických potřeb (musí být v souladu s rámcovým zadáním soutěžního rámce, tedy mohou zejména rozvíjet a upřesňovat Rámcový katalog služeb eGC).

Využití Portálu eGC

- Rychlé vytvoření zadávací dokumentace minitendru – využití metodik, vzorů, tržní nabídky a výsledků obdobných předchozích minitendrů.
- Rychlý nákupní proces v souladu se ZZVZ.

Implementace služeb eGC

- Služby budou mít definovány standardizované implementační nebo migrační procesy, proto jejich zřízení bude rychlé a migrační postupy dopředu známé.
- V případě selhání stávajícího provozovatele služeb KeGC bude možno rychle přejít k jinému provozovateli stejné služby. „Přesoutěžení“ služby bude rychlý a jednoduchý proces.

Používání služeb eGC

- Využití služeb eGC umožní v rámci rozvoje IS oddělit standardizované služby infrastruktury od vývoje a realizace změn aplikačního programového vybavení. Tento princip přispěje k rozbití „technologického vendor lock“ dodavatelů komplexních systémů typu „vertikální silo“, zahrnujících všechny vrstvy IS. Oddělení aplikačního vývoje od infrastruktury a využití služeb typu PaaS a SaaS v rámci vývoje aplikací přispěje ke standardizaci aplikací, zrychlí vývoj a umožní zadávání menších a časově méně rizikových veřejných zakázek.
- S využitím mechanismů pay-as-you-consume bude zákazník eGC používat a hradit pouze takový rozsah služeb, který bude požadovat aktuální provoz IS. Kapacity pro plánovaný rozvoj musí být zohledněny v zadání minitendru formou maximálních limitů čerpání, nicméně poté bude rychlost změn rozsahu čerpání záviset pouze na interním schvalovacím procesu daného zákazníka eGC.
- Bezpečnost a kvalita provozu služeb eGC je dána společně definovanými a aktualizovanými minimálními bezpečnostními a provozními standardy eGC.

Ukončení služeb eGC

- Součástí standardních smluvních podmínek jsou podmínky ukončení služeb včetně případné transitní ukončovací periody (převod dat, prokazatelné zničení dat, převod aplikačního kódu, ...).

6 Pohled provozovatele eGC

Tato kapitola uvádí požadavky a standardy závazné pro provozovatele eGC, společné pro obě části eGC. Standardy a opatření uvedené v této kapitole budou dále rozvíjeny ŘOeGC a průběžně aktualizovány.

Ověření souladu provozovatelů KeGC s požadavky na architektonické, provozní a bezpečnostní standardy bude provedeno v rámci hodnocení kvalifikace soutěžního rámce KeGC. Definice požadované dokumentace pro prokázání souladu provozovatele s požadavky bude součástí zadávací dokumentace soutěžního rámce KeGC a bude zohledňovat průmyslové certifikace a příslušné auditní zprávy, vyhotovené organizacemi k tomu akreditovanými v EU a EHS. ŘOeGC nebo zákazníci KeGC dále mohou požadovat tyto a další dokumentace, prokazující splnění požadavků na architektonické, provozní a bezpečnostní standardy, v rámci minitendru nebo v průběhu poskytování služby.

Ověření souladu provozovatelů SeGC s požadavky na architektonické, provozní a bezpečnostní standardy provádí ŘOeGC.

Úroveň naplnění standardů a opatření kvalifikovaných provozovatelů služeb KeGC a provozovatelů služeb SeGC budou publikovány na Portálu eGC.

6.1 Architektonické standardy

Architektura všech kategorií služeb (typu SaaS, PaaS i IaaS), nabízených poskytovatelem musí splňovat architektonické požadavky formulované v *Informační koncepci ČR* a v návazných dokumentech OHA – *Národní architektonický rámec, Národní architektonický plán*. Služby musí dodržovat všechny relevantní architektonické principy, uvedené v IKČR a všechny relevantní povinné návrhové architektonické vzory (Solution Patterns). Zejména musí dodržovat principy využívání centrálních služeb eGovernmentu, jako propojený datový fond (základní registry, eGSB), elektronické doručování (datové schránky), kontaktní místa (PVS, CzechPoint), správu identit (JIP/KAAS, NIA), kde jsou relevantní.

Provozovatel služeb eGC, zejména služeb typu SaaS, poskytne jako součást katalogu služeb architektonické informace v rozsahu požadovaném v žádosti o stanovisko OHA.

6.2 Bezpečnostní standardy a opatření

6.2.1 Místo uložení a zpracování dat

Strategie eGC se opírá o přístup založený na řízení rizik. Utajované informace dle zákona č. 412/2005 Sb. a stanovené druhy zpracování dat (IS zpravodajských služeb, IS bezpečnostních sborů související s plněním jim svěřených úkolů, a dále IS trestního a soudního řízení) nebudou využívat služby eGC. Zpracování informací a dat s nejvyšší úrovní dopadu bude probíhat v bezpečnostní úrovni 4 (Kritická), a bude omezeno na služby SeGC s místem uložení dat v ČR. Zpracování informací a dat v bezpečnostních úrovních 1-3 (Nízká, Střední, Vysoká) bude vyžadovat uložení dat v jurisdikci EU, a to prokázáním lokality jednoho nebo více datových center provozovatele KeGC na území členských států EU, a smluvním závazkem uložení dat na území EU. Přitom je třeba vzít v úvahu mnohem širší termín „zpracování dat“ dle definice v ZoOOÚ a v obecném nařízení GDPR, které zahrnuje i „nahlédnutí“ a „zpřístupnění přenosem“ (viz čl. 4 GDPR). Zpracování dat tedy zahrnuje i např. náhledy na provozní logy a jakékoli dálkové připojení uživatele a dočasné zobrazení dat na koncovém zařízení. Z toho důvodu je v níže uvedeném seznamu opatření i požadavek na ošetření případných zpracování dat mimo jurisdikci EU některým z nástrojů dle článků 44 až 47 obecného nařízení GDPR.

6.2.2 Bezpečnostní úrovně služeb eGC

Kapitola 5.2 popisuje metodiku určení úrovně bezpečnostních dopadů IS nebo jeho funkční části a její mapování na požadovanou bezpečnostní úroveň služeb eGC (kategorizace 1-4 – Nízká, Střední, Vysoká, Kritická). Tato kapitola popisuje bezpečnostní standardy a opatření, které musí implementovat provozovatel služeb eGC jednotlivých bezpečnostních úrovní. Definice požadovaných bezpečnostních opatření je založena na zavedených bezpečnostních standardech a prokázání účinnosti těchto opatření pomocí relevantních auditních zpráv.

Požadavky na bezpečnostní opatření odpovídající jednotlivým úrovním dopadů (1-4) jsou uvedeny a kategorizovány v následující tabulce. Tabulka vychází z požadavků následujících zákonů a norem, ve znění pozdějších předpisů a aktuálních verzí:

- ZoISVS – Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
- ZoKB – Zákon č. 181/2014 Sb., o kybernetické bezpečnosti
- Vyhláška 82/2018 Sb., o kybernetické bezpečnosti (VoKB)
- ZoOOÚ – Zákon č. 101/2000 Sb., o ochraně osobních údajů
- ZoOUI – Zákon č. 412/2005 Sb., o ochraně utajovaných informací
- ČSN ISO/IEC 27000 – Informační technologie – Systémy řízení bezpečnosti informací
- ČSN ISO/IEC 27001 – Požadavky
- ČSN ISO/IEC 27002 – Soubor postupů pro opatření bezpečnosti informací
- ČSN ISO/IEC 27017 – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002
- ČSN ISO/IEC 27018 – Soubor postupů na ochranu osobně identifikovatelných informací (PII) ve veřejných cloudech vystupujících jako zpracovatelé PII
- GDPR – Obecné nařízení o ochraně osobních údajů (General Data Protection Regulation)
- CSA – Cloud Security Alliance Best Practices for Mitigating Risks in Virtualized Environments
- Akční plán NBÚ k Národní strategii kybernetické bezpečnosti ČR 2015 až 2020
- ČSN ISO/IEC 20000 – Informační technologie – Management služeb

Poznámka: při *uplatňování ISO27000 a ZoKB/VoKB je navíc třeba důsledně odlišovat komplexní pohled bezpečnosti celého IS, využívajícího služby eGC, a vnitřní pohled provozovatele eGC.*

Tabulku bezpečnostních opatření je nutné interpretovat následujícím způsobem: Provozovatel služeb eGC příslušné bezpečnostní úrovně musí poskytovat služby splňující požadavky uvedené v tabulce (např. Uložení šifrovacích klíčů v HSM pro bezpečnostní úroveň 3 a 4, uvedená SLA dostupnosti). Provozovatel služeb eGC může poskytovat i služby s nižší úrovní bezpečnostních opatření (např. s uložením šifrovacích klíčů v SW, nižší úroveň dostupnosti). Zákazník si může vybrat na základě konkrétních bezpečnostních požadavků vyplývajících z analýzy rizik svého IS variantu služby optimální z pohledu bezpečnosti a ceny.

Rozsah bezpečnostních opatření služeb eGC dále závisí na typu služby eGC – služby vyšší úrovně (PaaS, SaaS) zahrnují více vrstev implementace (např. správa OS, vývojový cyklus aplikace) a tudíž je pro ně relevantní větší rozsah bezpečnostních opatření odpovídajícím těmto vrstvám (např. správa privilegovaných účtů OS, oddělení vývojového, testovacího a produkčního prostředí apod.).

Tabulka – Požadavky na bezpečnostní opatření odpovídající jednotlivým bezpečnostním úrovním

Popis opatření	Regulace/norma	N (1)	S (2)	V (3)	K (4)	Poznámka
Část „S" – Smluvní podmínky mezi zákazníkem a poskytovatelem služby eGC						
S.1 – Součástí smluvních podmínek je SLA, zahrnující úroveň dostupnosti (vazba na přílohu č. 5 *Minimální smluvní podmínky* a přílohu č. 4 *Metodika hodnocení bezpečnostních dopadů*)	ČSN ISO/IEC 27001 A.15	96,16%	99,45%	99,90%	99,99%	Poskytovatel služeb eGC musí nabízet služby v této úrovni SLA, avšak v případě požadavku zákazníka může v dané bezpečnostní úrovni nabízet alternativu služby s nižší nebo vyšší úrovní dostupnosti v SLA.
S.2 – Smlouva obsahuje závazek účinného zavedení bezpečnostních opatření v rozsahu dané bezpečnostní úrovně	ČSN ISO/IEC 27001 A.15, ZoISVS §5b	X	X	X	X	
S.3 – Deklarace místa uložení zákaznických dat v rámci jurisdikce EU	ČSN ISO/IEC 27001 A.9, A.11	x	X	X		Pokud by nastalo předání a zpracování dat (širší definice) mimo jurisdikci EU, provozovatel služby eGC objasní důvody předávání a aplikuje některý způsob ošetření dle nařízení GDPR čl. 44 až 47.
S.4 – Deklarace místa uložení zákaznických dat v rámci jurisdikce ČR	ČSN ISO/IEC 27001 A.9, A.11				X	Pro bezpečnostní úroveň „4" se vyžaduje uložení dat v jurisdikci ČR. Výjimkou mohou být případy dekompozice IS a s tím související scénáře hybridního cloudu, kdy funkční části IS s nižší bezpečnostní úrovní (1 až 3) mohou být uloženy v rámci jurisdikce EU.
S.5 – Smlouva uvádí způsob poskytnutí informací o zavedených bezpečnostních opatřeních	ČSN ISO/IEC 27001 A.15, ZoISVS §5b	X	X	X	X	Poskytovatel služeb eGC dá zadavatelům vhodným způsobem k dispozici zkrácený popis, jakým způsobem jsou bezpečnostní opatření realizována. Může být podmíněn uzavřením NDA.
S.6 – Smluvní podmínky jsou v souladu s požadavky na zpracovatele dle čl. 28 Obecného nařízení GDPR	GDPR + budoucí prováděcí předpisy	Nepoužije se	X	X	X	Uplatnit všeobecně. Většina IS bude zpracovávat osobní údaje a služby eGC publikované v katalogu eGC by na to měly být připraveny. V kategorii "nízká" nebude možné zpracovávat osobní údaje, viz kapitola 6.2
S.7 – Smlouva obsahuje povinnost informovat zákazníka eGC o bezpečnostních incidentech týkajících se daného zákazníka eGC, a spolupracovat při jejich zvládání	ČSN ISO/IEC 27001 A.16.1.2; VoKB č. 82/2018 Sb. Příloha 7 odst. i) bod 1.	X	X	X	X	
S.8 – Smluvní podmínky dodavatele mohou obsahovat požadavek uzavření NDA	ČSN ISO/IEC 27001 A.15		X	X	X	Poskytovatel duševního vlastnictví nebo jiného obchodního tajemství nabídne zadavateli text obvyklého recipročního NDA.
Část „N" – Dodavatel musí prokázat zavedení bezpečnostních opatření dle základních norem a předpisů, a to předložením podkladové dokumentace. Podkladová dokumentace může být v jazyce českém, slovenském nebo anglickém.						

N.1 – ČSN ISO/IEC 27001		část.	X	X	X	Pro úroveň „1“ pouze deklarací poskytovatele a popisem zavedených bezpečnostních opatření v doménách A7, A9, A12, A13, A15, A16, A18, se smluvní možností auditu zákazníkem služby. Pro úroveň „2“ jsou povinné všechny domény ISO s výjimkou A10 a A14. Pro úrovně „3“ a „4“ jsou povinné všechny domény daného ISO. Zavedení bezpečnostních opatření se prokazuje předložením „Prohlášení o aplikovatelnosti“ (výčet opatření v požadované struktuře) a příslušnou auditní zprávou od akreditované auditní společnosti v rámci EU.
N.2 – ČSN ISO/IEC 27017			X	X	X	Zavedení bezpečnostních opatření se prokazuje předložením „Prohlášení o aplikovatelnosti“ (výčet opatření v požadované struktuře) a příslušnou auditní zprávou od akreditované auditní společnosti v rámci EU.
N.3 – ČSN ISO/IEC 27018	Obecné nařízení GDPR		X	X	X	Uplatnit jako výběrové kritérium zákazníka eGC v případě zpracování osobních údajů. Zavedení bezpečnostních opatření se prokazuje předložením „Prohlášení o aplikovatelnosti“ (výčet opatření v požadované struktuře) a příslušnou auditní zprávou od akreditované auditní společnosti v rámci EU.
N.4 – ZoKB, vyhláška č. 82/2018 Sb. (VoKB)				X	X	eGC služby v úrovni „3“ musí splňovat požadavky kladené na „provozovatele“ a „významné dodavatele“ VIS dle ZoKB §3 a VoKB §2, a služby v úrovni „4“ musí splňovat požadavky na „provozovatele“ a „významné dodavatele“ KII a ISZS. Dodavatel prokáže v rámci kvalifikačních požadavků DNS způsob naplnění na něj aplikovatelných požadavků.
N.5 – Deklarace vhodného kodexu chování dle scénáře zpracování nebo certifikace dle GDPR	Dle doporučení ÚOOÚ v době účinnosti GDPR		X	X	X	Možnost uplatnit jako kvalifikační kritérium ze strany zadavatele v případě zpracování osobních údajů; bude upřesněno ve spolupráci s ÚOOÚ.
N.6 – ČSN ISO/IEC 20000					X	Uplatnit obdobně v případech, kdy zákazník eGC certifikuje celý systém na ISO 20000
Část „C“ – Dodavatel musí prokázat níže uvedené certifikace (předáním certifikátu nebo linkem na jeho online verzi) a audity (předáním celé auditní zprávy – může vyžadovat NDA ze strany dodavatele) v jazyce českém, slovenském nebo anglickém						
C.1 – Self-assessment dodavatele ČSN ISO/IEC 27001		X				Viz poznámka v řádku naplnění ISO 27001 výše.
C.2 – Certifikace ČSN ISO/IEC 27001	Důvodová zpráva k VoKB č. 82/2018		X	X	X	
C.3 – Certifikace ČSN ISO/IEC 27017			X	X	X	
C.4 - Certifikace ČSN ISO/IEC 27018			X	X	X	
C.5 – Certifikace ČSN ISO/IEC 20000					X	Uplatnit v případech kdy zákazník eGC certifikuje celý systém na ISO 20000

C.6 – Auditní zpráva SOC 1 (SSAE16/ISAE 3402) Type II nebo ekvivalent	ČSN ISO/IEC 27001 A.18, ZoKB/vyhláška č. 82/2018 Sb. §16			X	X	
C.7 – Auditní zpráva SOC 2 (AT101) Type II nebo ekvivalent	ČSN ISO/IEC 27001 A.18, ZoKB/vyhláška č. 82/2018 Sb. §16			X	X	
C.8 – Zpráva o penetračních testech nebo umožní zákazníkovi provedení vlastních penetračních testů	ČSN ISO/IEC 27001 A.18, A.12, ZoKB/vyhláška č. 82/2018 Sb. §25			X	X	Zpráva o penetračních testech dle NIST SP 800-115 nebo OWASP Top Ten Project apod., provedení akreditovanou společností pod některým etickým kodexem, např. www.crest-approved.org, nebo umožní zákazníkovi provedení vlastních externích penetračních testů
C.9 – Bezpečnostní prověrky administrátorů v kombinaci „T" a „D" nebo bezpečnostní způsobilost všech administrátorů dle §80-§87 zák. č. 412/2005 Sb.	ZoOUI č.412/2005 Sb.				X	Z důvodu agregace služeb KII ve státní části eGC
Část „U" – Dodavatel předá upřesnění realizace vybraných bezpečnostních opatření formou prohlášení a technické dokumentace (v jazyce českém, slovenském nebo anglickém)						
U.1 – Způsob zálohování dat a procedury pro vytváření záložních kopií	ČSN ISO/IEC 27001 A.12.3.1, ZoKB/vyhláška č. 82/2018 Sb. §10 (1 k)	X	X	X	X	Upřesnění realizace opatření
U.2 – Existence plánu pro BC/DR a zajištění geografické redundance dat, plán předat na vyžádání zákazníkovi eGC, případně pod NDA	ČSN ISO/IEC 27001 A.17, ZoKB/vyhláška č. 82/2018 Sb. §15			X	X	Upřesnění realizace opatření
U.3 – Rozhraní (API) pro předávání provozních záznamů (logů) minimálně pro vnitřní síťovou infrastrukturu relevantní pro danou eGC službu, pro kontrolu stavu virtuálních výpočetních prostředků a datových úložišť, a případně pro aplikace, pokud jsou součástí dané služby.			X	X	X	Upřesnění realizace opatření
U.4 – Provozovatel má zaveden systém sledování a vyhodnocování bezpečnostních událostí (např. SIEM) a umožní zpřístupnění prioritních událostí zákazníkovi				X	X	Upřesnění realizace opatření
U.5 – Opatření pro zajištění úrovně dostupnosti – použití nástroje nebo služby pro zvýšení odolnosti vůči útokům typu DoS/DDoS (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany)	ČSN ISO/IEC 27001 A.12.1.3., ZoKB/vyhláška č. 82/2018 Sb. §27;		X	X	X	Upřesnění realizace opatření

U.6 – Služby centra bezpečnostního dohledu 24x7x365 pro sledování, vyhodnocování a řešení bezpečnostních událostí (může představovat volitelnou službu za příplatek nebo může být splněno službou třetí strany)	ČSN ISO/IEC 27001 A.12.4., ZoKB/vyhláška č. 82/2018 Sb. §23			X	X	Upřesnění realizace opatření
U.7 – Vynucení šifrování protokolem HTTPS / TLS při externích přenosech, vyloučení možnosti fall-backu na protokol HTTP (bez šifrování)	ČSN ISO/IEC 27001 A.10.1.1	X	X	X	X	Upřesnění realizace opatření
U.8 – Ochrana dat šifrováním v úložištích v cloudové službě algoritmem publikovaným ve VoKB; v případě uložení šifrovacích klíčů mimo perimetr zákazníka, musí být klíče uloženy v HSM modulu úrovně ochrany FIPS 140-2 level 2 (nebo ekvivalent), který musí být pod správou povinné osoby (může představovat volitelnou službu za příplatek)	ČSN ISO/IEC 27001 A.10.1.2; Vyhláška č. 82/2018 Sb., příloha č. 4			X	X	Upřesnění realizace opatření
U.9 – Součástí služby musí být možnost silné (např. dvoufázové nebo dvou faktorové) autentizace uživatelů – popsat mechanismus.	ČSN ISO/IEC 27001 A.9.4.2; Vyhláška č. 82/2018 Sb., §19			X	X	Upřesnění realizace opatření
U.10 – Provozovatel služby eGC deklaruje a technicky objasní možnost průběžné replikace zákaznických dat do prostředí on-premise nebo do státní části eGC. Provozovatel dále umožní službu „bulk import/export dat“ pro import či export velkých objemů dat prostřednictvím zaslání šifrovaných paměťových médií.	ČSN ISO/IEC 27001 A.17, ZoKB/vyhláška č. 82/2018 Sb. §27		X	X	X	Upřesnění realizace opatření
U.11 – Provozovatel služby eGC předá popis realizace kontejnerové technologie. Její využití musí být v souladu s výsledky analýzy rizik s ohledem na hodnocení důvěrnosti zákaznických dat (63bezpečnostní technologie může snížit úroveň separace tenantů v cloudu)	ISO 27017 CLD 12.4.5			X	X	Upřesnění realizace opatření
Část „K“ – Bezpečnostní požadavky na komunikační sítě. Dodavatel splní technickým popisem a případně odkazem na prováděcí technickou dokumentaci.						
K.1 – Zajištění a registrace fixní IP adresy v CMS z důvodu whitelistingu		X	X	X	X	
K.2 – Podpora VPN dle podmínek připojení v katalogu služeb CMS		X	X	X	X	www.mvcr.cz , dále volba „eGovernment“, dále volba „Komunikační infrastruktura veřejné správy a Centrální místo služeb“, dále volba „CMS“.

K.3 – Dostupnost prostřednictvím NIX.CZ (SLA) nebo jiného peeringového uzlu v ČR		X	X	X	X	Prokázat peering v ČR pomocí www.peeringdb.com nebo jiným srovnatelným způsobem. Deklarovat šířku pásma [Gb/s], kterou má daný provozovatel do peeringového bodu k dispozici.
K.4 – Splnění podmínek pro připojení do projektu FENIX (viz https://www.nix.cz/cs/file/NIX_PRAVIDLA_FENIX) – požadavek na poskytovatele připojení	Akční plán NBÚ k Národní strategii kybernetické bezpečnosti ČR 2015 až 2020, C.3.12			X	X	
K.5 – Šifrované komunikace (TLS/VPN) přes Internet/NIX s využitím kryptografických algoritmů publikovaných ve VoKB.		X	X	X	X	

Oddělení zdrojů využívaných jednotlivými zákazníky služeb eGC

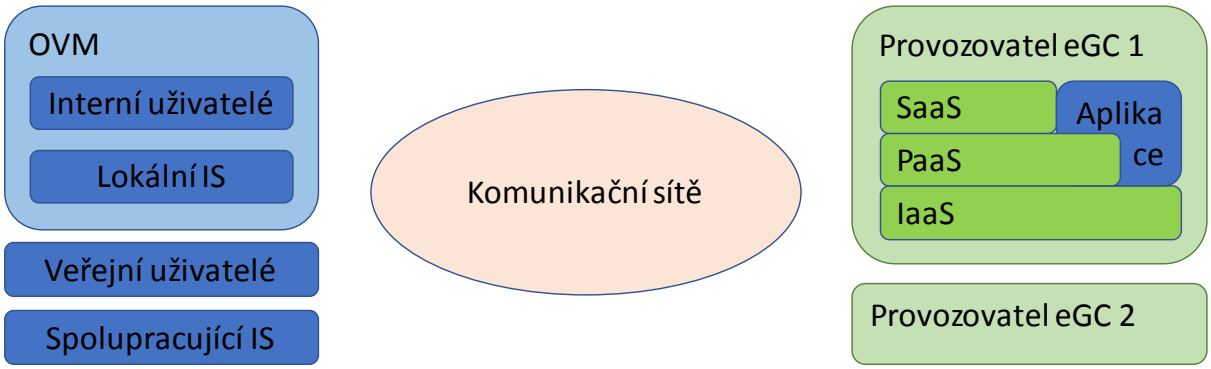
Provozovatel eGC musí oddělit zdroje využívané jednotlivými zákazníky tak, aby v případě narušení bezpečnosti jednoho zákazníka nedošlo k ohrožení ostatních zákazníků. Dále musí oddělit zdroje využívané zákazníky od zdrojů využívaných provozovatelem eGC k administraci služeb.

Takové oddělení zdrojů je obsahem požadavků ČSN ISO/IEC 27001 a ČSN ISO/IEC 27017

- A.13.1.3 – Princip oddělení v sítích
- A.13.1.2 – Segregation in computing environments
- A.12.3.1 – Zálohování informací

6.2.3 Kontext bezpečnostních opatření služeb eGC

Bezpečnostní opatření eGC jsou definována v kontextu celkové bezpečnosti implementace a provozu IS využívajícího služby eGC. Jednotlivé entity, účastnící se implementace a provozu takového IS, jsou ilustrovány na následujícím obrázku a jejich role v zajištění bezpečnosti IS je rozpracována níže.



6.2.4 Bezpečnostní opatření na straně uživatelů eGC

Na stranu uživatelů služeb eGC v tomto smyslu řadíme:

- interní uživatele (pracovníky) zákazníků eGC včetně administrátorů
- lokálně umístěné systémy, které komunikují s daným IS
- ostatní spolupracující systémy, které komunikují s daným IS
- veřejné uživatele IS
- aplikační vrstvu IS, případně i vrstvu provozu OS, provozované správcem IS nad PaaS a IaaS službami eGC

Bezpečnostní opatření na straně uživatelů a spolupracujících systémů jsou zcela v kompetenci správců jednotlivých IS, a vycházejí z aplikovatelné legislativy (ZoKB, ZoOOÚ, GDPR, …), norem (ČSN ISO/IEC 27000, ČSN ISO/IEC 20000, …), vnitřních politik a předpisů správce IS.

Z pohledu eGC lze formulovat pouze obecná doporučení, zejména v oblasti zabezpečení koncových stanic. Následující seznam oblastí není úplný. Vždy je třeba zvážit konkrétní případ a přihlédnout k infrastruktuře celé sítě, způsobu implementace jednotlivých technických řešení a také k procesům, které jsou v rámci dané organizace uplatňovány. Na níže uvedený seznam doporučení je nutné nahlížet ve smyslu zbytkových rizik, které zůstávají k mitigaci (ošetření, oslabení rizika) správcem IS – mimo oblast opatření vlastní cloudové služby, nebo ve sdílené odpovědnosti za optimální nastavení dané cloudové služby.

Doporučení – seznam oblastí, které mají vliv na celkovou míru zabezpečení stanic

1 SPRÁVA

1.1 HARDWARE a SÍŤ

- Oddělení koncových stanic do samostatné izolované podsítě (VLAN)
- Přehled HW a komu byl přidělen
- Definovat politiku BYOD a nepřipojovat je do stejného segmentu jako koncové stanice

1.2 SOFTWARE

- Pravidelné aktualizace
- Centrální správa
- Používat pouze podporované aplikace a OS
- Správná konfigurace aplikací/OS
- Zakázat/vypnout nevyužívané funkce

1.3 UŽIVATELÉ

- Centrální správa uživatelských účtů
- Definovaná a vynucená politika hesel
- Skupina Administrátorů
- Uživatelé nesmí používat administrátorské účty pro běžnou práci

1.4 UŽIVATELSKÁ DATA

- Na síťových discích ze serveru, ne na lokálních discích

2 ZABEZPEČENÍ

2.1 OBECNÁ NASTAVENÍ

- Omezení oprávnění uživatelů
- Omezení možnosti spouštění programů a skriptů
- USB zařízení
- Nastavená pravidla jejich použití
- Povolení pouze schválených USB zařízení
- Omezení možnosti spouštění programů

2.2 PŘIHLAŠOVÁNÍ

- Zakázat automatické přihlášení
- Využívat více faktorovou autentizaci

2.3 OCHRANA PŘED ZNEUŽITÍM STROJE

- Nastavit unikátní heslo BIOS
- Povolit bootování pouze z lokálního disku počítače
- Nastavení automatického uzamknutí účtu při nečinnosti
- Poučení uživatelů

2.4 OCHRANA PŘED ÚTOKY

- Antivirus
- Pravidelné aktualizace virových definic
- Firewall
- Pravidelná revize pravidel

- HIDS/HIPS
- Používání VPN (pro stroje mimo síť organizace)

2.5 DATA

- Šifrování disků
- Data loss prevention system

3 MONITORING a UCHOVÁNÍ LOGŮ

3.1 OBECNÉ ZÁSADY

- Na základě informací z monitorovacích nástrojů (zejména pro monitoring sítě) možnost dohledat konkrétní koncový stroj
- Centrální vyhodnocování a uchovávání
- Časová synchronizace

3.2 VYHODNOCOVÁNÍ INFORMACÍ

- Pravidelné
- Korelace informací ze všech dostupných zdrojů
- Nástroje nasazené na koncových stanicích
- Síťové prvky

3.3 UCHOVÁNÍ DAT pro POTŘEBY POZDĚJŠÍ ANALÝZY

- Alespoň 12 měsíců (v závislosti na dostupných zdrojích, zejména velikosti úložiště)

4 NASAZENÍ NOVÝCH STANIC

4.1 JEDNOTNÝ OBRAZ pro VŠECHNY STROJE

- Heslo účtu administrátora nového systému nesmí být stejné pro všechny stroje
- Operační systém a aplikace pravidelně aktualizovány

5 ZÁLOHOVÁNÍ

5.1 UŽIVATELSKÁ DATA

- Záloha serveru, odkud se připojují uživatelské disky

Testování obnovení dat ze zálohy

Z formulace požadavků na bezpečnostní opatření provozovatelů eGC vyplývají následující vodítka pro zákazníky eGC:

Popis opatření	Regulace/norma	N (1)	S (2)	V (3)	K (4)
Zákazník eGC poskytne součinnost pro bezpečnostní monitoring připojení do Centrálního místa služeb (CMS) prostřednictvím služby SOCR Ministerstva vnitra. Tato služba je poskytována s.p. NaKIT jako součást bezpečnostních opatření systému CMS, není odpovědností poskytovatele eGC služby.	ČSN ISO/IEC 27001 A.12.4., ZoKB/vyhláška č. 82/2018 Sb. §23, §24; ZoISVS §6g	X	X	X	X
SLA dostupnosti přes KIVS/CMS nesmí být horší než celková dostupnost služby eGC	ZoISVS §6g(4)	96,16%	99,45%	99,90%	99,99%

6.2.5 Bezpečnostní a provozní opatření na straně komunikačních sítí

Bezpečnostní opatření eGC jsou na oblast komunikačních sítí přímo aplikovatelná s ohledem na bezpečnostní perimetr a síťové rozhraní služeb eGC. Uživatelé služeb eGC pak musí použít takové přístupové metody, které jsou kompatibilní s bezpečnostními požadavky perimetru služeb eGC, zejména připojení s odpovídajícím SLA.

Seznam konkrétních bezpečnostních opatření či požadavků na komunikační sítě, využívané k připojení zákazníka eGC do dané cloudové služby, je uveden v posledním oddílu tabulky bezpečnostních opatření výše.

Požadavky na připojení do služby CMS 2.0

S ohledem na znění §6g odst. (3) a (4) zák. č. 365/2000 Sb., a dále v souladu s metodickými pokyny připojení služeb IS do Centrálního místa služeb (CMS) na webu MV (http://www.mvcr.cz/clanek/komunikacni-infrastruktura-verejne-spravy-a-centralni-misto-sluzeb-584441.aspx) stanovujeme tyto minimální provozní a bezpečnostní požadavky na služby KeGC (které budou využívat služeb CMS 2.0):

- Služba KeGC musí mít pevnou IP adresu, kterou lze zařadit do whitelistingu na CMS 2.0.
- Služba KeGC musí podporovat některou z metod zabezpečení VPN tunelováním, a to dle technických podmínek služby připojení „CMS2 – 08 – Přístup do CMS“ v aktuálním katalogu služeb CMS.
- Služba KeGC bude mít dostatečnou úroveň zabezpečení svých výpočetních zdrojů s ohledem na zpracovávaná aktiva proti kybernetickým útokům zneužití dat přenášených z / do CMS neautorizovaným přístupem.
    - Služby IS umístěné v KeGC, které využívají pouze funkce **čtení dat** z ISZR nebo eGSB, budou zařazeny minimálně do bezpečnostní úrovně „**střední**“.
    - Služby IS umístěné v KeGC, které využívají funkcí **čtení i zápis dat** z/do ISZR nebo eGSB, budou zařazeny minimálně do bezpečnostní úrovně „**vysoká**“.

Poznámka: CMS má zajištěnou vysokokapacitní redundantní konektivitu do NIX.CZ.

Komentář k tabulce bezpečnostních opatření – zapojení se do projektu FENIX: Provozovatelé eGC nebo jejich poskytovatelé připojení musí splnit podmínky pro připojení do projektu FENIX, jako například redundantní připojení, provoz 7x24 NOC, filtrování zdrojových adres apod. (viz https://www.nix.cz/cs/file/NIX_PRAVIDLA_FENIX). Vlastní připojení do projektu FENIX, který umožňuje v případě masivních kybernetických útoků oddělenou komunikaci mezi důvěryhodnými sítěmi na platformě NIX.CZ, je provozovatelům eGC doporučeno – v souladu s Akčním plánem k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, C.3.12: „Podporovat projekt Fénix a zapojení významných sítí veřejné správy za účelem zachování funkcionalit a služeb během masivních kybernetických útoků“.

6.2.6 Bezpečnostní dohled

DCeGOV je Dohledové centrum eGovernmentu, služba bezpečnostního dohledu, kterou poskytuje jako správce Ministerstvo vnitra, přičemž provozováním této služby může pověřit jiný subjekt.

Pasívní bezpečnostní dohled eGC

Pasívním bezpečnostním dohledem eGC rozumíme bezpečnostní vyhodnocování signálů a logů z komponent, které implementují služby eGC a CMS. Jde tedy o „vnitřní“ dohled služeb eGC ze strany provozovatelů služeb a CMS, bez aktivní spolupráce se správci IS.

DCeGOV provádí pasívní bezpečnostní dohled nad provozem CMS a služeb státní části eGC jako povinnou součást služeb státní části eGC. Provozovatelé služeb státní části eGC mají povinnost napojení na DCeGOV a podporu implementace a provozu těchto služeb DCeGOV.

DCeGOV dále provádí pasívní bezpečnostní dohled CMS jako brány do veřejného Internetu, a tím i pasívní dohled připojení správce IS ke službám komerční části eGC, pro něž je CMS ve funkci poskytovatele služeb připojení do Internetu. V případě hrozících nebo zjištěných bezpečnostních incidentů a událostí v rozsahu relevantním pro zajištění bezpečnosti CMS a služeb komerční části eGC se DCeGOV obrací primárně na správce IS, neboť správce je nejlépe schopen vyhodnotit, zda se skutečně jedná o bezpečnostní incident či jen o provozní anomálii. V případě hrozících bezpečnostních incidentů nebo zjištěných zranitelností se DCeGOV může obracet i přímo na provozovatele komerčních služeb eGC, avšak se zohledněním míry odpovědnosti a smluvních závazků, sjednaných mezi správcem IS a daným provozovatelem, případně mezi správcem IS a DCeGOV.

Provozovatelé komerční části eGC musí jako součást služeb eGC poskytovat služby pasívního bezpečnostního dohledu a související služby v rozsahu podle bezpečnostní úrovně dané služby, v souladu s tabulkou bezpečnostních opatření eGC.

V závislosti na bezpečnostní úrovni služeb eGC musí DCeGOV a provozovatelé služeb eGC správci IS poskytovat:

- rozhraní (API) pro předávání provozních záznamů služeb (logů) správcům IS – povinné pro bezpečnostní úrovně 2, 3 a 4,
- systém vyhodnocování bezpečnostních událostí a zpřístupnění prioritních událostí správcům IS – povinné pro bezpečnostní úrovně 3 a 4,
- služby centra bezpečnostního dohledu 24x7x365 pro sledování, vyhodnocování a řešení bezpečnostních událostí v koordinaci se správcem IS – volitelná služba pro bezpečnostní úrovně 3 a 4.

DCeGOV a provozovatelé služeb eGC tedy musí poskytnout svým zákazníkům dostatek informací a součinnost při vyhodnocování a řešení bezpečnostních událostí a zvládání bezpečnostních incidentů, v rozsahu závisejícím na bezpečnostní úrovni služeb eGC. Provozovatelé služeb eGC jsou dále regulováni v rámci stávající legislativy – ZoKB a ZoISVS ve znění pozdějších předpisů.

V souvislosti s pasívním bezpečnostním dohledem DCeGOV a provozovatelů komerční části eGC mají správci IS za povinnost ustanovit komunikační kanály s DCeGOV na operativní úrovni a vzájemně se s DCeGOV informovat o hrozících nebo zjištěných bezpečnostních incidentech a událostech v rozsahu relevantním pro zajištění bezpečnosti CMS a služeb eGC. Stejně tak musí provozovatelé komerčních služeb uvést svoje kontakty pro technickou podporu a hlášení bezpečnostních incidentů v rámci Katalogu eGC služeb tak, aby v případě potřeby mohl DCeGOV upozornit na hrozby i přímo daného provozovatele komerční služby.

Aktivní bezpečnostní dohled eGC

Aktivním bezpečnostním dohledem eGC rozumíme bezpečnostní vyhodnocování signálů a logů z komponent IS využívajících služby eGC, které správci IS volitelně zpřístupní za účelem bezpečnostního dohledu. Jde tedy o dohled IS využívajícího eGC (např. Dohled aplikačních komponent běžících nad PaaS službami), který vyžaduje spolupráci správce IS (předávání logů, stanovení pravidel vyhodnocování).

DCeGov poskytuje služby aktivního bezpečnostního dohledu systému CMS.

Služby aktivního dohledu eGC (státní i komerční části) může správci IS poskytovat DCeGov jako volitelnou službu, správce IS ji může provozovat interně nebo zadat třetí straně. Správce IS musí v každém případě naplnit požadavky ZoKB a ZoISVS v rozsahu aplikovatelném na jeho systém.

Služby aktivního bezpečnostního dohledu DCeGov budou uvedeny v katalogu služeb eGC jako služby SeGC. Mezi služby KeGC mohou být uvedeny za předpokladu, že jejich poskytovatel má oddělené účetnictví, že mají transparentní nákladovou strukturu, a že nedochází k nedovolené státní podpoře, která by mohla narušit fungující trh.

Součástí definice služeb bezpečnostního dohledu budou i požadavky na rozhraní pro předávání logů a provozních informací, na komunikační kanály správce IS s DCeGOV na operativní úrovni a vzájemné informování o hrozících nebo zjištěných bezpečnostních incidentech a událostech v rozsahu relevantním pro zajištění bezpečnosti daného IS a relevantních služeb eGC.

6.2.7 Udržitelnost ochranných opatření, stanovených právními předpisy pro bezpečnostní sbory a zpravodajské služby

V rámci standardů a řízení eGC budou zachovány, případně analogicky uplatněny aktuální mechanismy spolupráce s bezpečnostními sbory a zpravodajskými službami v souladu s ustanoveními příslušných zákonů a podzákonných předpisů, mj.

- evidenční ochrana údajů - § 11 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, §§ 140 a 141 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, § 35 zákona č. 341/2011 Sb., o Generální inspekci bezpečnostních sborů, § 59 zákona č. 17/2012 Sb., o Celní správě České republiky, ve znění pozdějších předpisů,
- krycí prostředky a krycí doklady - §§ 7, 13 zákona č. 154/1994 Sb., o Bezpečnostní informační službě, ve znění pozdějších předpisů, §§ 7 a 13 zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, § 18 zákona č. 153/1994 Sb., o zpravodajských službách České republiky, ve znění pozdějších předpisů, § 75 zákona č. 273/2008 Sb., o Policii České republiky, ve znění pozdějších předpisů, § 40 zákona č. 17/2012 Sb., o Celní správě České republiky, ve znění pozdějších předpisů, § 42 zákona č. 341/2011 Sb., o Generální inspekci bezpečnostních sborů,
- opatřeních k dopadům elektronizace veřejné správy na činnost bezpečnostních sborů a zpravodajských služeb – bod 2 písm. B) a bod 3 písm. C) Usnesení vlády ČR č. 343/D ze dne 6. května 2015, o opatřeních k dopadům elektronizace veřejné správy na činnost zpravodajských služeb a bezpečnostních sborů České republiky a o použití a změně zvláštních postupů k utajení a zajištění bezpečnosti při správě daní a pojistných a registraci smluv o důchodovém spoření.

V rámci poskytování služeb eGC musí být podporovány následující mechanismy:

- Zákazník eGC může pro vybrané služby zřídit administrátorské účty (na úrovni oprávnění dostupných zákazníkovi služeb eGC) pro použití bezpečnostních sborů a zpravodajských služeb, který jim umožní přístup k logům,
- Pokud zákazník eGC provozuje aplikaci s ochrannými opatřeními (na úrovni aplikačního vybavení) dle výše uvedených předpisů, jsou opatření aplikovatelná on-premise stejná v eGC,
- Pokud jsou pro IS stanovena související organizační ochranná opatření (např. Zpracování nebo předávání některých logů), musí být zachována při použití služeb eGC,
- Ve schvalovacích a kontrolních procesech ŘOeGC budou zohledněna uvedená ochranná opatření a spolupráce se zástupci bezpečnostních sborů a zpravodajských služeb.

6.3 Provozní standardy

Provozní standardy zahrnují procesy a nástroje, jejichž primárním cílem je zajištění konzistentní kvality služby a komunikace se zákazníkem. Typicky jsou založeny na frameworku ITIL nebo ISO 20000, nástroje zahrnují monitoring, ServiceDesk apod. Certifikace ISO 20000 je v tabulce bezpečnostních opatření uvedena jako požadavek na provozovatele SeGC. Pro provozovatele KeGC byl zvolen jiný přístup k definici a kontrole provozních standardů eGC. Vzhledem k tomu, že kvalita provozních procesů a nástrojů se přímo odráží v dodržování SLA, byl zvolen přístup zpětné kontroly a řízení prostřednictvím SLA místo detailní definice provozních procesů a nástrojů a jejich proaktivního auditu.

Dále budou stanoveny minimální požadavky na rozhraní provozních procesů a nástrojů z pohledu zákazníků eGC.

6.3.1 Koncept hrubého porušení SLA

ŘOeGC definuje koncept hrubého porušení SLA, který bude zakotven v minimálních smluvních podmínkách KeGC. Hrubé porušení SLA bude definováno na základě míry nesplnění standardních SLA služeb, paralelně k sankcím za porušení těchto SLA. Hrubá porušení SLA budou evidována u ŘOeGC.

V případě hrubého porušení SLA bude mít zákazník právo na okamžitou výpověď smlouvy s tím, že provozovatel uhradí náklady migrace služeb k jinému provozovateli (tyto náklady musí být ze strany zákazníků eGC explicitně vyčísleny už v momentě poptávky služeb eGC).

V případě opakovaného hrubého porušení SLA pro různé zákazníky bude poskytovatel vyloučen ze soutěžního mechanismu KeGC.

Detailnější popis konceptu hrubého porušení SLA je zahrnut v příloze č. 5 *Minimální smluvní podmínky*.

6.3.2 Rozhraní provozních procesů a nástrojů pro zákazníky

ŘOeGC stanoví minimální standardy pro rozhraní a způsob komunikace se zákazníkem v níže uvedených oblastech:

- technická podpora – komunikace o incidentech a dalších provozních událostech,
- měření dostupnosti s ohledem na místo dodání služby, plánované odstávky služby,
- reporting stavu služby,
- možnost načítání provozních a bezpečnostních událostí pro další zpracování zákazníkem,
- podklady pro vyúčtování.

Prvotní návrh těchto standardů je zahrnut v příloze č. 5 *Minimální smluvní podmínky*.

6.4 Minimální smluvní podmínky

ŘOeGC stanoví minimální smluvní podmínky služeb eGC. Minimálními smluvními podmínkami jsou rozuměny takové smluvní podmínky, které musí splnit každý dodavatel služeb eGC (v soutěžním mechanismu KeGC jsou součástí zadávacích podmínek). při nákupu služeb KeGC je zadavatelům minitendrů (zákazníkům eGC) doporučeno držet se těchto smluvních podmínek. Zákazník eGC může požadovat v minitendru striktnější nebo jinak strukturované smluvní podmínky, vystavuje se ale riziku, že neobdrží žádné nabídky nebo obdrží nestandardní nabídky za vyšší než očekávané ceny.

Minimální smluvní podmínky jsou stanoveny v následujících oblastech

- dostupnost služby,
- podpora služby,
- měření dostupnosti,
- místo dodání,

- vyhodnocení dostupnosti a penalizace,
- možnost předčasného ukončení smlouvy,
- ukončení smlouvy a sankce v případě hrubého porušení SLA,
- reportování.

ŘOeGC dále stanoví obecně pro využití služeb KeGC tyto povinné oblasti a podmínky, které je nutné zahrnout do smlouvy s dodavatelem nebo poskytovatelem služby:

- Kvalifikační podmínky soutěžního rámce by měly být přeneseny do smlouvy se sankcemi při porušení – obvyklé je zneplatnit smlouvu při nedodržení kvalifikačních podmínek soutěžního rámce v průběhu trvání smlouvy.
- Zákazníci eGC, kteří budou využívat služeb KeGC v rámci systémů spadajících pod ZoKB, se s ohledem na charakter zpracování dat v cloudu a určení svých „významných dodavatelů“ budou muset řídit požadavky novelizované vyhlášky č. 82/2018 Sb. (VoKB), která v příloze č. 7 uvádí sadu smluvních požadavků na významné dodavatele.

Prvotní návrh minimálních smluvních podmínek je v příloze č. 5 *Minimální smluvní podmínky*.

7 Právní rámec KeGC

Pro realizaci soutěžního mechanismu a nákupních procesů KeGC byl zvolen soutěžní mechanismus DNS (Dynamický nákupní systém). DNS je upraven v § 138 – 142 ZZVZ. DNS je jedním z velmi flexibilních nástrojů pro zadávání veřejných zakázek. Jedná se o plně elektronizovanou formu zadávání veřejných zakázek. Zadavatel po zavedení DNS může zadávat zakázky aktuálně podle svých momentálních potřeb. V průběhu trvání DNS je zároveň možné zasahovat do zadávací dokumentace, na jejímž základě byl DNS zaveden a která je po celou dobu jeho trvání uveřejněna na profilu zadavatele. Je tedy možné v době trvání DNS například aktualizovat předmět veřejných zakázek, které mají být v rámci DNS zadávány, podle vývoje potřeb zadavatele nebo aktualizovat zadávací podmínky, například podle vývoje obecných bezpečnostních standardů. Délka zavedeného DNS není nijak omezena.

Velmi podstatnou náležitostí dynamického nákupního systému je jeho otevřenost pro dodavatele. V tom je jeden ze základních rozdílů oproti rámcovým dohodám, kde je vyloučena možnost přístupu dalších dodavatelů. V době trvání DNS je možné rozšiřovat nejen okruh dodavatelů, kteří mohou podávat žádosti o účast i po jeho zavedení, ale i okruh zadavatelů, kteří budou dynamický nákupní systém využívat.

Jednotlivé „soutěžní rámce KeGC“ budou realizovány samostatnými DNS, pro realizaci návazných „soutěžních rámců KeGC“ lze využít i mechanismus aktualizace předmětu a podmínek účasti předchozího DNS.

Centrálním zadavatelem bude v souladu s kompetenčním zákonem Ministerstvo vnitra. Centrální zadavatel prostřednictvím ŘOeGC vytvoří a bude spravovat Portál eGC, který bude sloužit jako informační centrum pro potenciální dodavatele i zadavatele. Portál eGC bude obsahovat mimo jiné i tzv. Katalog služeb eGC, resp. Rámcový katalog služeb eGC, který bude mít roli předmětu zadání, tedy informaci pro potenciální zadavatele, kteří by chtěli přistoupit do zavedeného DNS, o rozsahu a charakteru služeb, které mají být v DNS pořizovány.

Dynamický nákupní systém se zavádí pro pořizování běžného a obecně dostupného zboží, služeb nebo stavebních prací. Cloudové služby obecně jsou vzhledem ke svému sdílenému charakteru principiálně komoditními službami. Komoditní charakter služeb eGC je dále posílen jejich jednotnou definicí a popisem v Rámcovém katalogu eGC. Kritérium běžnosti a obecné dostupnosti služeb je třeba vzít v úvahu při zpracování Rámcového katalogu eGC.

Zákon umožňuje rozdělení dynamického nákupního systému do kategorií, které odpovídají konceptu „částí soutěžního rámce KeGC“. Tyto kategorie se odvozují od předmětu veřejné zakázky, mohou to být tedy například kategorie dodávek podle předem vymezených skupin zboží. Rozdělení dynamického nákupního systému na kategorie tedy může využít zadavatel zejména tehdy, pokud dojde k závěru, že pro každou kategorii by mohl existovat samostatný okruh dodavatelů. při rozdělení podle předmětu lze uvést jako příklad kategorie na jednotlivé IT komponenty, resp. cloudové služby. Pro každou kategorii pak zadavatel stanoví vlastní podmínky účasti, obdobně jako u rozdělení veřejné zakázky na části.

Pro zavedení DNS se použijí přiměřeně pravidla pro užší řízení, to znamená, že zadavatel posuzuje splnění podmínek účasti ještě před podáním nabídek. Přestože je užší řízení koncipováno jako řízení dvoufázové, v případě zavedení DNS bude použita pouze první fáze. Zavedení DNS tedy probíhá formou výzvy neomezenému počtu dodavatelů k podání žádostí o účast. V žádostech o účast dodavatelé prokazují splnění podmínek účasti stanovených zadávacími podmínkami. Zadavatel posoudí soulad těchto žádostí se zadávacími podmínkami. Zákon stanovuje výslovně povinnost vyloučit ty účastníky zadávacího řízení, jejichž žádosti nesplňují zadávací podmínky. Pokud účastník zadávacího řízení podmínky splnil, je zařazen do DNS. V této fázi tedy neprobíhá žádné hodnocení nabídek, neboť nejsou ze strany dodavatelů předkládány žádné údaje k hodnocení.

Katalog tržní nabídky služeb KeGC a procesy jeho naplnění včetně vlastního institutu informace o nabídce služeb dodavatele neodpovídají žádnému institutu v rámci DNS dle ZZVZ, a proto je nutné realizovat je jinou doplňující metodou, např. tržní konzultací.

Samotné zadávání veřejných zakázek v DNS („minitendrů KeGC“) se pak řídí zvláštními procesními pravidly, neboť nejde o zadávací řízení, ale o tzv. Zvláštní postup, kdy zadavatel zasílá výzvu k podání nabídek všem dodavatelům, kteří jsou zařazeni do DNS. Pokud je systém rozčleněn do kategorií, zadavatel vyzývá pouze dodavatele zařazené v příslušné kategorii. Náležitosti výzvy jsou uvedeny v příloze č. 6 ZZVZ. Výzva musí obsahovat alespoň identifikační údaje zadavatele, údaje o přístupu k zadávací dokumentaci, lhůtu pro podání nabídek, způsob podání nabídek včetně informace o tom, v jakém jazyce mohou být podány a pravidla pro hodnocení nabídek.

Po obdržení nabídek zadavatel provede jejich hodnocení podle kritérií uvedených ve výzvě k podání nabídek. Pro hodnocení nabídek se v případě DNA dynamického nákupního systému použijí obecná pravidla pro hodnocení. Po výběru dodavatele odešle zadavatel těm dodavatelům, kteří jsou zařazeni do DNS a zároveň podali nabídku, oznámení o výběru. Zároveň si zadavatel od vybraného dodavatele vyžádá předložení dokladů o kvalifikaci, pokud už je nemá k dispozici, tedy pokud již v rámci DNS byla vybranému dodavateli zadána veřejná zakázka a před podpisem smlouvy již doklady předložil, nebo doklady předložil při zavádění DNS či při přístupu do něj z vlastní iniciativy nebo na základě požadavku zadavatele na objasnění nebo doplnění údajů, dokladů, vzorků nebo modelů dle § 46 odst. 1 ZZVZ.

Lze tedy shrnout, že pokud se jedná o cloudové služby, definované v tomto dokumentu jako ICT prostředky (výpočetní zdroje, úložiště, aplikace) a související služby poskytované typicky vzdáleně prostřednictvím komunikačních sítí jako služba externího poskytovatele s definovanými parametry kvality, realizovaná na sdílených platformách pro více uživatelů (multi-tenant), IaaS služby, definované jako pronájem virtuálních HW zdrojů, PaaS služby, definované jako poskytování výpočetní infrastruktury spolu se standardními SW platformami jako jsou operační systémy, databáze, webové a aplikační servery a SaaS služby, definované jako poskytování kompletní aplikační funkcionality jako služby dostupné po síti, jeví se jako možné pořizování těchto služeb prostřednictvím DNS.

8 Právní rámec SeGC

V průběhu Fáze I. Projektu *Příprava vybudování eGovernment cloudu* bylo identifikováno několik variant řešení právního rámce státní části, které do různé míry naplňují jednotlivá stanovená kritéria. Varianty jsou uvedeny v tomto dokumentu s rozborem jejich nevýhod a rizik, provedeným pracovní skupinou RVIS pro přípravu vybudování eGC.

Legislativní rozpracování variant řešení právního rámce, včetně koncepčního zadání souvisejících změn legislativy a doporučení jedné z variant bude provedeno meziresortní komisí garantů jednotlivých relevantních zákonů – MV (ZoISVS), MF (ZoRP), MPO (ZoSP) a MMR (ZZVZ) – ve spolupráci s pracovní skupinou RVIS pro přípravu vybudování eGovernment cloudu na základě požadavků, kritérií a variant uvedených v tomto dokumentu (SAZ). Termín předložení legislativního rozboru a doporučené varianty vládě je do 30.6.2019. Koncepční zadání legislativních změn bude podkladem pro úkoly v usnesení Vlády ČR pro jednotlivé ministry.

8.1 Východiska pro posuzování variant

V souladu s principy, pravidly a dalšími koncepty eGC uvedenými v tomto dokumentu jsme pro posuzování jednotlivých variant zvolili následující kritéria:

- Soulad se ZZVZ a ZoRP.
- Nákup standardizovaných sdílených služeb z elektronického katalogu přes Portál eGC – základní princip eGC zajišťující nákladovou a cenovou efektivitu provozu IS.
- Možnost využití všemi resorty a jimi zřizovanými organizacemi i ostatními ústředními orgány státní správy.
- **Majetkový status a úroveň řízení státem** – ovládáno/řízeno státem, v majetku státu, zákaz vendor lock - vychází z bezpečnostních požadavků na SeGC, určeného pro umístění a provoz IS nejvyšší bezpečnostní úrovně.
- **Zapojení stávajících státních ICT podniků**, využití investovaných prostředků, zajištění kontinuity aktuálně poskytovaných služeb. Možnost zaměstnání ICT expertů mimo tabulkové platy (a služební zákon). Předpokládaný model zapojení státních ICT podniků je rozdělení služeb po technologických vrstvách (DC, sítě, HW, aplikace, dohledy) spíš než podle částí katalogu služeb.
- **Nekonkurence poskytovatelů SeGC** – zaručuje nezdvojování a efektivní využití investic a zdrojů, eliminuje rizika využití nedovolené podpory v konkurenci. Vyžaduje alternativní mechanismy kontroly cenové úrovně SeGC prostřednictvím ŘOeGC.
- **Přímý komerční vztah (smlouva)** zákazníka eGC s provozovatelem SeGC, což umožňuje platby za služby eGC z rozpočtu zákazníka eGC a zároveň zajišťuje přímou motivaci k efektivnímu čerpání služeb (neplýtvání) a nepřímou motivaci k nákladové efektivitě služeb SeGC (tlak zákazníků, přímo prostřednictvím smluvního jednání nebo prostřednictvím ŘOeGC). Komerční smluvní vztah s SLA a sankcemi dále umožňuje řízení kvality služeb. Modely čerpání „zadarmo“ (financování rozpočtovou alokací) obsahují významné riziko zkreslování poptávky a cenové efektivity dodávek a jsou nekompatibilní s řešením KeGC (riziko narušení trhu KeGC – neopodstatněné kategorizace IS do nejvyšší bezpečnostní úrovně z finančních důvodů).
- **Kompatibilita s právním rámcem KeGC, zamezení narušení hospodářské soutěže** – zejména stejný princip přímého komerčního vztahu, jasné vymezení pravidel umístění IS do KeGC a SeGC.
- Zachování in-house výjimky (Vertikální spolupráce dle § 11 ZZVZ) zakladatelů stávajících státních ICT podniků– ohrožení výjimky v momentě, kdy služby SeGC pro ostatní zákazníky eGC překročí hranici 20%.
- Možnost použití v přechodné době bez změny zákonů.

- **Rychlost realizace dané varianty –** čím déle bude trvat realizace zvolené varianty, tím déle budou trvat nedostatky stávajícího stavu dotčených IS (nedostatečná opatření pro zajištění požadované bezpečnosti IS; provozování IS na nesdílených platformách, které vede k nižšímu využití SW, HW i lidských zdrojů; vysoké náklady provozovaných IS)

Obecná rizika z pohledu ZZVZ:

Vzhledem k tomu, že všechny diskutované varianty právního rámce SeGC mají charakter úplné či částečné výjimky ze ZZVZ, je nutno dostatečně konkrétně vymezit kritéria pro využití služeb SeGC, tj. jednak kritéria hodnocení bezpečnostní úrovně 4 a jednak kontrolní mechanismy, zda jsou tato kritéria správně aplikována. Z hlediska ZZVZ se může jevit jako rizikové možné podřazení služeb, které by měly spadat do úrovně 1 až 3, pod úroveň 4, která má speciální režim, čímž by mohlo hrozit riziko obcházení ZZVZ a narušení hospodářské soutěže. Toto riziko je ošetřeno přesnou definicí bezpečnostní úrovně 4 (viz kapitola 5.2 tohoto dokumentu), kontrolou hodnocení bezpečnostních dopadů pro systémy bezpečnostní úrovně 4 minimálně na úrovni ŘOeGC a určením seznamu IS k umístění do SeGC v nařízení Vlády ČR nebo zákonem.

Všechny varianty kromě varianty Standardních veřejných zakázek obsahují riziko monopolního chování provozovatele služeb SeGC a vzniku ekonomické neefektivity na straně nabídky. Z toho důvodu je nutno implementovat efektivní kontrolu nákladové efektivity služeb SeGC prostřednictvím ŘOeGC, jak je popsáno v tomto dokumentu.

8.2 Nový státní podnik pro SeGC zřízený zákonem

Samostatným novým zákonem nebo novelizací zákona ZoISVS bude založen nový státní podnik pro poskytování služeb SeGC. Navrhovaný název podniku je **Státní centrum eGC (SCeGC).** Nový státní podnik bude společně řízen všemi resorty a jeho řídící struktury budou definovány tak, aby odpovídaly požadavkům § 11 ZZVZ (Vertikální spolupráce) na ovládající veřejné zadavatele.

(3) Veřejní zadavatelé společně ovládají právnickou osobu podle odstavce 1 písm. a), pokud

a) orgány s rozhodovacím oprávněním takto ovládané právnické osoby jsou složeny nebo ustaveny na základě jednání ve shodě všech společně ovládajících veřejných zadavatelů,

b) ovládající veřejní zadavatelé mají společně rozhodující vliv na strategické cíle a významná rozhodnutí takto ovládané právnické osoby a

c) takto ovládaná právnická osoba nesleduje žádné zájmy, které jsou v rozporu se zájmy ovládajících veřejných zadavatelů.

Nový státní podnik bude dále zákonem pověřen poskytováním služeb SeGC takovým způsobem, aby pro nákup služeb SeGC mohli ostatní veřejní zadavatelé využít výjimky dle § 29 odst. q) ZZVZ.

[Zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení,] jde-li o veřejnou zakázku na služby zadávanou veřejným zadavatelem jinému veřejnému zadavateli nebo několika veřejným zadavatelům na základě výhradního práva přiznaného právním předpisem nebo uděleného na základě právního předpisu.

Vymezení rozsahu poskytovaných služeb SeGC bude určeno na úrovni zákona výčtem IS, které budou umístěny do SeGC jako celek nebo bude do SeGC umístěna jejich část. Tento výčet bude sestaven na základě metodiky hodnocení bezpečnostních dopadů stanovené v této souhrnné analytické zprávě. Seznam bude pravidelně aktualizován formou novelizace zákona a při vzniku nových agendových zákonů může být doplňován. Legislativní řešení musí umožnit zohlednění časování umístění jednotlivých IS do SeGC z hlediska termínů udržitelnosti

stávajících investic do technologické infrastruktury, termínů udržitelnosti z hlediska čerpaných dotací EU a termínů obnovy nebo významného rozšíření technologické infrastruktury – například formou nařízení vlády, stanovujícího termíny umístění IS na seznamu do SeGC.

Nový státní podnik vznikne převodem a sloučením částí majetku (zejména technologické infrastruktury) a organizačních struktur sávajících ICT podniků, relevantních pro poskytování služeb SeGC. Stávající ICT podniky zůstanou zachovány a budou poskytovat svým zakladatelům služby mimo SeGC. Legislativní řešení musí umožnit kontinuitu provozu stávajících komplexních systémů provozovaných státními ICT podniky po dobu jejich finanční a technologické udržitelnosti i po převedení technologické infrastruktury od nového státního podniku.

Pracovní skupina RVIS pro přípravu vybudování eGC doporučila tuto variantu.

Posouzení z pohledu ZZVZ:

Tato varianta byla formulována v průběhu meziresortního připomínkového řízení a nebyla posouzena ze strany MMR. Řada stanovisek formulovaných pro ostatní varianty je ale aplikovatelná v příslušném rozsahu i pro tuto variantu.

Nevýhody a rizika varianty:

- Časování – je nutná příprava nového zákona nebo novelizace ZoISVS.
- Riziko neshody mezi ovládajícími resorty ve státním podniku – lze diskutovat i podvariantu s jedním ovládajícím subjektem a využití výjimky § 29 odst. q) ZZVZ jako primárního nástroje zadávání zakázek.
- Dělení státních ICT podniků, zejména v případě SPCSS (datová centra, HW serverových a diskových platforem), přináší krátkodobá rizika vnitřní stability státních ICT podniků i nového podniku.

8.3 Sloučený státní ICT podnik založený Vládou ČR a ovládaný všemi resorty

Sloučením existujících státních ICT podniků vznikne nový státní podnik pro poskytování služeb SeGC. Zakladatelem takového státního podniku by byla Vláda ČR jako nejvyšší exekutivní orgán státu, případně Úřad vlády ČR, a členy dozorčí rady by byli zástupci jednotlivých ministerstev. Tím by bylo zabezpečeno „ovládání“ podniku prostřednictvím Vlády ČR a zástupců svých resortů jednotlivými organizačními složkami státu v pozici veřejného zadavatele, tudíž by bylo umožněno využití „in-house výjimky“ ZZVZ (Vertikální spolupráce dle § 11 ZZVZ).

Řešení vyžaduje novelizaci zákona o státním podniku, která definuje statut státního podniku zřízeného vládou a jeho společného ovládání všemi ministerstvy. Tímto postupem by bylo umožněno zadávat zakázky všemi OSS (primárně ministerstvům a prostřednictvím nich také jimi zřizovaným organizacím) na in-house výjimku.

Vznik jednoho centrálního státního podniku ovládaného a kontrolovaného vládou by vyřešilo nejen odstranění často duplicitního a neefektivního poskytování služeb více existujícími státními podniky, ale také by došlo ke zjednodušení řídící úrovně více státních podniků.

Posouzení z pohledu ZZVZ:

K aplikaci spolupráce na vertikální úrovni dle ustanovení § 11 ZZVZ (výjimka in – house dle předchozí právní úpravy) je nutné splnění dvou základních podmínek, a to kritéria kontroly a kritéria výkonu činnosti. Pro naplnění první podmínky (kritéria kontroly) je nutno, aby veřejný zadavatel stoprocentně vlastnil subjekt, s nímž chce smlouvu uzavřít. Jakákoliv majetková účast soukromého subjektu by toto kritérium jednoznačně vyloučila. Současně je nezbytné, aby veřejný orgán jako zadavatel vykonával nad dotčeným odlišným subjektem obdobnou kontrolu jako je ta, kterou vykonává nad svými organizačními jednotkami. Existuje také možnost

společné kontroly, a to, že kontrolu může vykovávat několik zadavatelů společně, přičemž v takovém případě jsou všichni oprávněni aplikovat vertikální spolupráci.

K existenci kritéria kontroly není rozhodující samotný způsob, jakým je prováděna. Obecně se však pro naplnění tohoto kritéria vychází zejména z hlediska existence výlučného vlastnictví předmětného subjektu ze strany veřejného subjektu a samozřejmě je nutno zkoumat i konkrétní způsob, jakým je kontrola vykonávána. Pokud je shledána existence výlučného vlastnictví, je nutno dále zkoumat, zdali tento subjekt, kterému má být zakázka zadána, je fakticky ovládán veřejným zadavatelem, a to ve smyslu existence rozhodujícího vlivu veřejného zadavatele na strategické cíle a významná rozhodnutí právnické osoby, blíže viz rozhodnutí SDEU ve věci C – 182/11 Econord, dle kterého je kritérium kontroly naplněno v případě, kdy ovládající veřejný zadavatel disponuje v ovládané osobě jak účastí majetkovou, tak účastí v jejích řídících orgánech.

K existenci kritéria výkonu činnosti je požadováno, aby více než 80% celkové činnosti takto ovládané osoby bylo prováděno při plnění úkolů, jež jí byly svěřeny ovládajícím zadavatelem. Pro určení podílu činností podle § 11 odst. 1 písm. C) ZZVZ se bere v úvahu průměrný obrat, pokud je činnost, která je předmětem smlouvy, hrazena jejími příjemci v plné výši. Není-li možno určit tento obrat, použijí se jako základ pro výpočet v případě vertikální spolupráce celkové náklady právnické osoby. Pro určení podílu činnosti v rámci vertikální spolupráce jsou v rámci tohoto ustanovení zakotvena podrobnější pravidla, a to pro stanovení konkrétního podílu činnosti v případě, kdy ovládaná právnická osoba musí pro zadavatele vykonávat více než 80 % činnosti, která je realizována při plnění úkolů, jež jí byly svěřeny zadavatelem.

Pokud vycházíme ze shora uvedených premis ke kritériu kontroly, a to existence rozhodujícího vlivu veřejného zadavatele na strategické cíle a významná rozhodnutí ovládaného subjektu, je pro tyto účely nezbytné, aby bylo vymezeno, kdo bude správcem rozpočtové kapitoly, kdo bude jmenovat generálního ředitele, schvalování vnitřního uspořádání či výkon odborného dohledu nad činností podniku. V tomto případě má být zakladatelem Úřad vlády ČR a v dozorčí radě mají být zástupci jednotlivých ministerstev, kde je nezbytné, aby měli fakticky rozhodující vliv na strategické cíle a významná rozhodnutí ovládaného subjektu, tento je z hlediska judikatury SDEU charakterizován především jako účast majetková a účast v řídících orgánech ovládaného subjektu.

Pokud tedy kromě Úřadu vlády ČR budou moci jednotliví zástupci ministerstev zasahovat do chodu podniku v takové míře, že podnik nebude schopen činit např. Významná hospodářská rozhodnutí, či obdobná rozhodnutí zásadního vlivu bez jejich souhlasu, bylo by lze konstatovat, že by mohla být shledána existence rozhodujícího vlivu veřejných zadavatelů nad strategickými cíli a významnými rozhodnutími ovládaného subjektu a tedy podmínka ovládání nezbytná pro aplikaci ustanovení § 11 ZZVZ, obdobně by tedy i bylo lze presumovat splnění podmínky výkonu činnosti ve výši více než 80% činnosti pro tyto veřejné zadavatele.

Nevýhody a rizika varianty:

- Časování – je nutná novelizace zákona o státním podniku a pravděpodobně i ZoISVS.
- Budoucí rozhodovací praxe ÚOHS či příslušných soudů, kterou nelze presumovat, například z důvodu rizika spočívajícího ve faktickém splnění podmínky kritéria kontroly.
- Riziko neshody mezi zastupujícími resorty ve státním podniku.

8.4 Realokace rozpočtů a poskytování služeb SeGC prostřednictvím zakladatelů státních ICT podniků

Služby SeGC jsou u státních podniků objednávány jejich zakladateli a poskytovány ostatním zákazníkům eGC zdarma (model Základní registry). Financování realokací odpovídajících prostředků z rozpočtových kapitol zákazníků eGC do rozpočtových kapitol MF a MV.

Posouzení z pohledu ZZVZ

Tato varianta má nejnižší rizika z pohledu ZZVZ, neboť vůbec neobsahuje zadávání veřejných zakázek a z tohoto pohledu jde o variantu preferovanou MMR.

Nevýhody a rizika varianty:

- Neexistence komerčního vztahu zákazníka a provozovatele, čerpání služeb SeGC „zadarmo“ se všemi výše uvedenými dopady – riziko plýtvání na straně poptávky, riziko cenové neefektivity na straně nabídky, nepřímé řízení kvality, rizika narušení trhu KeGC. Alternativní kontrolní mechanismy prostřednictvím ŘOeGC by byly velmi složité a pravděpodobně neúčinné.
- Přestože jde o model aktuálně používaný např. V oblasti služeb datových schránek nebo základních registrů, v tomto případě by šlo o realokaci řádově vyšších a poměrně významných finančních prostředků a jejich administrativní řízení vyžaduje náročné meziresortní plánování a dává velký prostor pro neefektivitu a klientelismus.
- Vyžaduje změny kompetenčního a rozpočtových zákonů, bez přechodového období.
- Neodpovídá přirozenému rozdělení činností mezi státními ICT podniky – řešitelné sloučením podniků, což ale okamžitě ruší in-house výjimku jednoho ze stávajících zakladatelů.

8.5 Sdružení státních ICT podniků a výjimka dle § 29 odst. q) ZZVZ

Provozovatelem státní části eGC bude sdružení stávajících státních ICT podniků. Zákazníci eGC budou nakupovat služby eGC od provozovatele SeGC na základě výjimky v § 29 odst. q) zákona č. 134/2016 Sb., o zadávání veřejných zakázek („ZZVZ“).

§ 29 odst. q) ZZVZ stanoví, že:

[Zadavatel není povinen zadat veřejnou zakázku v zadávacím řízení,] jde-li o veřejnou zakázku na služby zadávanou veřejným zadavatelem jinému veřejnému zadavateli nebo několika veřejným zadavatelům na základě výhradního práva přiznaného právním předpisem nebo uděleného na základě právního předpisu.

Výklad § 29 odst. q) ZVVZ nepřipouští, aby takové výhradní právo bylo uděleno více osobám. EU směrnice o zadávání veřejných zakázek uvádí v odst. (30) explicitněji, že:

V určitých případech může být daný veřejný zadavatel či dané sdružení veřejných zadavatelů jediným zdrojem dané služby, na jejíž poskytování má výhradní právo v souladu s právními a se zveřejněnými správními předpisy, jež jsou slučitelné se Smlouvou o Fungování EU.

Právními předpisy, které upraví výhradní právo poskytovat služby státní části eGC, mohou být:

1) krátkodobě – „cloudová“ vyhláška NÚKIB

a) Nová vyhláška NÚKIB připravovaná podle § 6 e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti („ZoKB“) definuje obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu (tzv. „cloudová vyhláška NÚKIB“). Vyhláška je připravována v souladu s metodikou hodnocení bezpečnostních dopadů a s definicí bezpečnostních opatření eGC. Pro bezpečnostní úroveň dopadů 4 (Kritická) bude obsahovat požadavek provozu v datových centrech a na HW a SW platformách v majetku státu a provozu organizacemi řízenými státem (OSS nebo státní podniky). Z tohoto bezpečnostního požadavku vyplývá potřeba Státní části eGC.

b) Vyhláška může dále určit za poskytovatele služeb SeGC konkrétní osobu – sdružení stávajících státních ICT podniků nebo jejich společný podnik. Obecně může jít o sdružení nebo společný podnik všech státních ICT podniků, které splní bezpečnostní a provozní požadavky bezpečnostní úrovně 4 (Kritická), založené za účelem poskytování služeb SeGC.

2) dlouhodobě – novela ZoISVS, případně i budoucí novelizace ZoKB

Dlouhodobě se použití výjimky § 29 odst. q) ZZVZ bude opírat primárně o novelizované znění ZoISVS a případně i o novelizované znění ZoKB. Tím bude eliminováno potenciální riziko napadení využití vyhlášky jako nedostatečně silného (podzákonného) právního předpisu pro omezení ZZVZ.

Posouzení z pohledu ZZVZ:

Pro účely této výjimky musí být výhradní právo zakotveno právním předpisem – a to zákonem, či podzákonným právním předpisem, jež je prováděcím předpisem k zákonu, který věcně řeší danou problematiku. Pokud by se mělo jednat o výhradní právo přiznané či udělené podzákonným právním předpisem, příslušný zákon musí obsahovat zmocnění k vydání takového podzákonného předpisu.

V případě navrhované vyhlášky k zák. č. 181/2014 Sb., o kybernetické bezpečnosti, která by zakotvila za poskytovatele služeb SeGC konkrétní subjekty, které splní bezpečnostní a provozní požadavky bezpečnostní úrovně–4 – kritická, lze konstatovat, že ZZVZ zakotvuje podmínku stanovení výhradního práva právním předpisem, bez ohledu na to, zda se jedná přímo o zákon či podzákonný právní předpis. Vzhledem k závažnosti a rozsahu daného projektu lze však jen doporučit zakotvení výhradního práva přímo zákonem.

Je však nutno zdůraznit, že právní předpis, jímž bude státním podnikům založeno či přiznáno výhradní právo, musí splňovat podmínku jeho souladu s právem EU, a to dle čl. 11 směrnice 2014/24/EU, o zadávání veřejných zakázek. Tuto skutečnost, a to kompatibilitu s právem EU je nutno ověřit na Úřadu Vlády –R – odboru kompatibility, a to z důvodu, že při navrhovaném postupu lze spatřovat významné riziko, spočívající v obcházení zejména soutěžního práva EU z hlediska vytvoření umělého monopolního stavu.

Nevýhody a rizika varianty:

- Varianta nabízí relativně rychlou možnost realizace v dočasném období, kompatibilita tohoto krátkodobého řešení s doporučenou variantou dlouhodobého řešení musí být důkladně posouzena.
- Úprava vyhlášky NÚKIB podle bodu 1b) zatím nedojednána, pokud nedojde ke shodě, bude nutno čekat na novelizaci ZoISVS.
- Kompatibilita právního předpisu zakotvujícího výhradní právo státním podnikům z hlediska souladu s právem EU.
- Budoucí rozhodovací praxe ÚOHS a příslušných soudů, zejména ve vztahu k druhu právního předpisu, jímž má být výhradní právo stanoveno a dále riziko obcházení soutěžního práva.
- Do budoucna nemusí být splněny podmínky pro aplikaci vertikální spolupráce dle ustanovení § 11 ZZVZ ve vztahu ke zakladatelům státních podniků.

8.6 Akciová společnost ovládaná všemi resorty

Je obdobou varianty centrálního státního ICT podniku s tím že nový podnik by měl statut akciové společnosti, ve které každý resort drží alespoň jednu akcii.

Posouzení z pohledu ZZVZ

K možnosti tohoto řešení lze odkázat na obecné vymezení podmínek pro aplikaci ustanovení § 11 ZZVZ v kapitole 8.2, a to kritéria kontroly a kritéria výkonu činnosti. k tomuto návrhu řešení lze odkázat na rozhodnutí SDEU, a to konkrétně rozhodnutí SDEU ve věci–C – 182/11 Econord, dle kterého je kritérium kontroly naplněno v případě, kdy ovládající veřejný zadavatel disponuje v ovládané osobě jak účastí majetkovou, tak účastí v jejích řídících orgánech, a dále rozhodnutí ve věci C-340/04 Carbotermo v případě založení akciové společnosti by tedy za předpokladu, že by každý resort disponoval minimálně jednou akcií společnosti a zároveň měl účast v řídících orgánech společnosti, měly by být naplněny podmínky pro aplikaci vertikální spolupráce dle ustanovení § 11 ZZVZ.

Nevýhody a rizika varianty:

- Tato varianta je možná bez úpravy zákonů, nicméně je výrazně komplikovanější z hlediska řešení majetkového statutu a zajištění kontinuity stávajících státních ICT podniků.
- Výhodou varianty centrálního státního ICT podniku proti této variantě je taky fakt, že formálně stanovený způsob ovládání podniku (vládou jako celkem) přesněji odpovídá reálnému stavu věci, zatímco držení relativně malé části akcií neodpovídá reálnému vlivu, který budou jednotlivé resorty schopny uplatňovat prostřednictvím vlády.
- Riziko neshody mezi akcionáři.
- Budoucí rozhodovací praxe ÚOHS či příslušných soudů, kterou nelze presumovat, například z důvodu rizika spočívajícího ve faktickém splnění podmínky kritéria kontroly

8.7 Standardní veřejné zakázky

Jednotliví zákazníci eGC vypisují standardní veřejné zakázky na služby SeGC na základě metodiky publikované ŘOeGC. Povinným požadavkem soutěží jsou bezpečnostní požadavky bezpečnostní úrovně 4, tj. Provozovatelé jsou ovládáni státem a služby provozují na majetku státu.

Nevýhody a rizika varianty:

- Uvedený bezpečnostní požadavek významně zkresluje skutečný soutěžní charakter veřejných zakázek. Soutěže se účastní pouze státní podniky, případně státní akciové společnosti.
- Riziko nedodržování standardů katalogu SeGC a snížení celkové efektivity SeGC.
- Narušení principu nekonkurence poskytovatelů SeGC.

9 Pohled ŘOeGC

Kapitola definuje kompetence a role ŘOeGC, z velké části odkazuje na již dříve definovaná témata, která prezentuje z pohledu ŘOeGC.

9.1 Organizační struktura a zařazení

Řídící orgán eGC bude v souladu s kompetenčním zákonem umístěn na MV, bude ustanoven jako samostatný útvar, ale bez vlastního administrativního zázemí (tj. ne samostatný úřad nebo OSS). ŘOeGC bude spolupracovat zejména s odbory OHA a OKB v rámci sekce informačních a komunikačních technologií MV a odborem OVZ v rámci sekce ekonomiky a provozu MV. V době před zřízením samostatného útvaru pověří ministr vnitra výkonem kompetencí ŘOeGC některý z existujících útvarů MV.

Role ŘOeGC je principiálně meziresortní, ŘOeGC bude pracovat v úzké vazbě na RVIS. Pro ŘOeGC bude zřízen meziresortní poradní orgán složený ze zástupců Ministerstva vnitra, Ministerstva financí a NÚKIB, zástupců zpravodajských služeb, zástupců ústředních orgánů státní správy, zástupců orgánů veřejné správy a zástupců odborné veřejnosti. Jednotlivé resorty při nominace členů poradního orgánu vezmou v úvahu kontinuitu projektu Příprava vybudování eGovernment cloudu.

Ve schvalovacích a kontrolních procesech ŘOeGC bude zohledněna spolupráce se zástupci bezpečnostních a zpravodajských služeb, viz kapitola 6.2.7.

Návrh počátečního personálního obsazení ŘOeGC má následující strukturu:

Pozice	FTE (ekvivalent plné pracovní doby)
Vedoucí/Project Manager	1
Metodik standardů (včetně právní podpory)	2
Správce katalogu služeb	1
Nákupní oblast	2
Architektura	1
Quality Assurance	1

Jednorázové provozní náklady na vybavení a zřízení ŘOeGC jsou odhadovány ve výši 1,6 mil. Kč.
Roční personální náklady včetně povinného pojištění a FKSP (s trvalým vlivem) jsou odhadovány výši 12,6 mil. Kč.
Roční provozní náklady (s trvalým vlivem) včetně externích expertních služeb jsou odhadovány ve výši 5,9 mil. Kč.

Zdrojem financování ŘOeGC je státní rozpočet.

9.2 Metodické řízení eGC

Primární úlohou ŘOeGC bude metodické řízení eGC. Úlohou ŘOeGC je rozpracovat a rozvíjet principy popsané v tomto dokumentu a poskytovat zákazníkům eGC metodickou podporu pro jejich použití, včetně metodických pokynů, praktických příkladů, školení apod.

9.3 Sběr dat a řízení celkové migrace do eGC

ŘOeGC:

- Zajistí vytvoření aplikace pro správu katalogu DC veřejné správy tak, aby tento katalog byl schopen uchovávat informace potřebné pro řízení eGC.
- Zajistí novou verzi ISoISVS, tak, aby tento katalog byl schopen uchovávat informace potřebné pro řízení eGC.
- Pravidelně (minimálně 1x ročně) kontroluje plnění a změny katalogu aktuálně provozovaných IS. V případě, že s některými údaji nesouhlasí (to se týká zejména údajů TCO a údaje o zařazení komponenty do jedné ze čtyř úrovní požadované bezpečnosti, projedná tyto údaje se správcem. Případné neshody řeší ŘOeGC s pomocí svého poradního orgánu a v další instanci ministr vnitra s příslušným ministrem nebo statutárním zástupcem příslušného ústředního orgánu.
- Na základě informací z katalogů identifikuje vhodné kandidáty ICT služeb, které budou nabízeny zákazníkům eGC ze SeGC a z KeGC.

9.4 Řízení SeGC

ŘOeGC:

- Na základě schválených požadavků věcných správců IS na využití služeb státní části eGC (uložených v ISoISVS) určí potřebnou kapacitu datových center státu zařazených do SeGC v jednotlivých časových obdobích (a to včetně záloh).
- Určí seznam, kapacity a služby DC zařazených do SeGC pro dané období. při této činnosti ŘOeGC postupuje tak, aby využil zdroje stávajících DC SeGC a současně pokryl, pokud možno všechny požadavky zákazníků eGC na využití služeb SeGC.
- Ověří soulad služeb provozovatelů SeGC s bezpečnostními a provozními požadavky eGC pro bezpečnostní úroveň 4 (Kritická).
- Na základě oprávněných požadavků věcných a technických správců dohodne s provozovateli SeGC jejich ICT služby (jejich vzorová SLA a jejich jednotkové nabídkové ceny) a tyto služby ověří (certifikuje). Poté služby zveřejní na portálu eGC, a to ve stejné struktuře jakou mají katalogy služeb KeGC.
- Provádí kontrolu cenové úrovně SeGC.
- Vytvoří harmonogram pro migraci IS do SeGC.
- Monitoruje migraci služeb do SeGC a monitoruje provoz služeb SeGC.

9.5 Řízení KeGC

ŘOeGC:

- Plánuje a vypisuje soutěžní rámce KeGC.
- Vytvoří a na Portálu eGC publikuje Katalog eGC.
- Monitoruje migraci služeb do KeGC a monitoruje provoz služeb KeGC.

9.6 Portál eGC

ŘOeGC:

- Bude správcem IS Portálu eGC.
- Vytváří a dále rozvíjí Portál eGC tak, aby byl efektivním nástrojem jak pro správce IS, tak pro provozovatele SeGC a KeGC.

9.7 Pilotní projekty

ŘOeGC bude řídit pilotní projekty dle plánu v kapitole 10

- Pilotní projekt Portálu eGC
- Pilotní projekt KeGC
- Pilotní provoz SeGC

10 Plán vybudování eGC

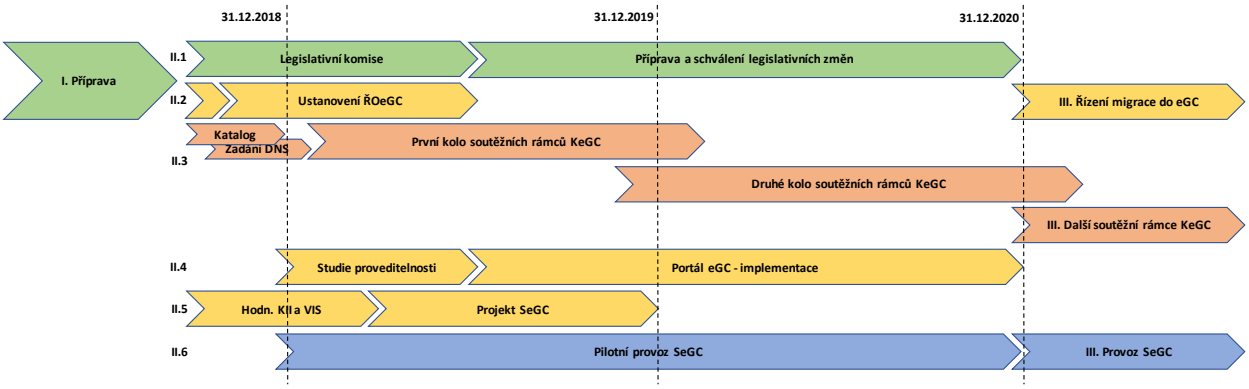
10.1 Celkový časový plán

Dokument *Strategický rámec Národního cloud computingu - eGovernment cloud ČR* rozděluje přípravu a vybudování eGC na tři hlavní fáze:

- **Fáze I. (přípravná)** – aktuální fáze, ve které probíhal projekt „Příprava vybudování eGovernment cloudu“ (dle strategického rámce 2016-2017, reálně 2016-2018**),**
- **Fáze II. (pilotní,** v dřívějších materiálech nazývána realizační) – postupné vybudování eGC sadou pilotních projektů (dle strategického rámce 2018-2020),
- **Fáze III. (standardizační)** – standardizace IS v eGC (2021 a dále).

Fáze II. je navržena tak, aby realizaci eGC bylo možné zahájit bez změn legislativy. Pro třetí fázi projektu bude třeba upravit legislativní rámec tak, aby bylo možné využít ekonomické efektivity, transparentnosti a dynamičnosti trhu s cloudovými službami v plném rozsahu.

Tato kapitola upravuje a rozpracovává tyto fáze, zejména Fázi II do sady paralelních dílčích fází.



Fáze I. - přípravná

- Příprava komplexní Souhrnné analytické zprávy (tento dokument - SAZ), která bude předložena Vládě ČR ke schválení.
- Schválení Souhrnné analytické zprávy a usnesení Vlády ČR s úkoly pro období do schválení legislativních změn.

Fáze II.1 – příprava a schválení legislativních změn

Viz plán legislativních změn v kapitole 10.2.

Poznámka: součástí je naplnění úkolu C.7.03 *Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období 2015 až 2020* “Zmapovat současný stav a případně vypracovat návrh legislativních změn s ohledem na vytvoření státního cloudu včetně datových úložišť“.

Termíny:

- **Do 30.11.2018 –** ministr vnitra ve spolupráci s ministryní financí, ministryní průmyslu a obchodu a ministryní pro místní rozvoj ustanoví meziresortní komisi pro legislativní rozpracování variant řešení právního rámce státní části SeGC, včetně koncepčního zadání souvisejících změn legislativy a doporučení jedné z variant, ve spolupráci s pracovní skupinou RVIS pro přípravu vybudování eGC a na základě požadavků, kritérií

a variant uvedených v souhrnné analytické zprávě (meziresortní komise garantů relevantních zákonů).

- **Do 30.6.2019** – meziresortní komise předloží vládě toto legislativní rozpracování a koncepční zadání legislativních změn garantům příslušných zákonů ve formě návrhu usnesení vlády.
- **Cca 2 roky** – příprava a schválení legislativních změn.

Fáze II.2 – ustanovení ŘOeGC

Viz kapitola 9.1.

Termíny:

- **Do 31.10.2018** - ministr vnitra pověří některý útvar ministerstva vnitra dočasným výkonem kompetencí ŘOeGC a ustanoví poradní orgán složený ze zástupců Ministerstva vnitra, Ministerstva financí a NÚKIB, zástupců zpravodajských služeb, zástupců ústředních orgánů státní správy, zástupců orgánů veřejné správy a zástupců odborné veřejnosti.
- **Do 30.6.2019** - ministr vnitra ustanoví ŘOeGC jako samostatný útvar ministerstva vnitra.

Fáze II.3 – pilotní projekt KeGC

- Příprava a vypsání dvou pilotních soutěžních rámců (DNS) v oblastech IaaS (zaměřeno primárně na OSS) a SaaS (zaměřeno primárně na samosprávu). Definice úvodní omezené sady služeb s potenciálním velkým dopadem na cílové skupiny.
- Pro OSS bude pilotní fáze zaměřena na podporu migrace zejména agendových systémů do bezpečných datových center KeGC. Půjde proto zejména o služby housingu, IaaS a PaaS.
- Pro malé a střední obce bude pilotní fáze zaměřena především na jejich provozní IS (tzv. back-end systémy), ve kterých existuje v současné době jak největší multiplicita provozovaných systémů, tak největší riziko bezpečnosti provozu IS. Proto pilotní fáze bude pro tyto typy zákazníků eGC zaměřena na služby SaaS (ERP, HR, spisová služba, apod.).
- Příprava i propagace služeb KeGC v aktivní spolupráci se zákazníky (Svaz měst a obcí, RVIS, …).

Termíny:

- **Do 31.12.2018** - sestavení první verze Rámcového katalogu služeb eGC a příprava prvních soutěžních rámců (DNS). Provede ŘOeGC a jeho poradní orgán.
- **Do 31.1.2019** – příprava zadávacích podmínek prvního DNS KeGC. Provede ŘOeGC a jeho poradní orgán ve spolupráci s OVZ MV.
- **Q1 2019** – vypsání prvního kola soutěžních rámců (DNS).
- **2020** – vypsání druhého kola soutěžních rámců (DNS).

Fáze II.4 – pilotní projekt Portálu eGC

- Studie proveditelnosti, výběr a otestování nástrojů, funkční specifikace a odhad nákladů realizace Portálu eGC. Odhadované náklady na realizaci studie proveditelnosti jsou ve výši 1,1 mil. Kč.
- Implementace Portálu eGC. Odhadované náklady implementace budou určeny ve studii proveditelnosti.

Termíny:

- **Q1-Q2 2018** – vypracování studie proveditelnosti. Provede ŘOeGC. Navazuje na sestavení první verze Rámcového katalogu služeb eGC (Fáze II.3).

- **Cca 2 roky** – implementace Portálu eGC. Provede ŘOeGC.

Fáze II.5 – projekt státní části eGC - sběr informací od potenciálních zákazníků eGC a detailní stanovení konkrétních plánů ekonomických, kapacitních a plánu migrace

- Sběr informací formou cílených a statistických průzkumů,
- ohodnocení bezpečnostních dopadů jednotlivých IS jejich správci,
- doplnění kalkulace TCO pro stávající IS,
- sběr informací o provozovaných platformách HW/OS,
- sběr informací o předpokládaném termínu obnovy HW,
- příprava detailního a konkrétního celkového ekonomického pohledu, celkového kapacitního plánu pro vybudování SeGC (technické i personální kapacity) a celkového plánu migrace IS do eGC,
- analýza předpokládaných finančních dopadů na státní rozpočet případně na veřejné rozpočty a financování z fondů ESIF,
- analýza dopadů využití služeb eGC na personální kapacity zákazníků eGC (snížení potřeby provozních IT pracovníků atd.).

Poznámka: Tato fáze je zároveň naplněním úkolu C.7.02 *Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období 2015 až 2020* "Vypracovat a vládě předložit projekt státního cloudu včetně datových úložišť a další potřebné podklady (finanční, bezpečnostní, organizační a technické nároky)"

Termíny:

- **31.3.2019** – ústřední orgány státní správy, spravující kritické a významné ISVS dle ZoKB zpracují hodnocení bezpečnostních dopadů a kalkulaci TCO pro tyto ISVS v jejich resortech podle metodik uvedených v tomto dokumentu (SAZ) a předají je včetně informací o termínech udržitelnosti investic do těchto ISVS jako podklady ŘOeGC.
- **31.12.2019** – ŘOeGC zpracuje projekt státní části eGovernment cloudu včetně kapacitních, finančních a organizačních plánů.

Fáze II.6 – pilotní provoz SeGC

- Příprava katalogu služeb SeGC. Navazuje na sestavení první verze Rámcového katalogu služeb eGC (Fáze II.3).
- Vybudování prvních služeb SeGC ve spolupráci státních ICT podniků, využívání služeb SeGC v systémech resortů MF a MV, případně i dalších na základě aktuálně dostupných mechanismů v souladu se ZZVZ (vertikální a horizontální spolupráce).

Fáze III. – po schválení legislativních změn

- Implementace finálního právního rámce SeGC - založení centrálního státního ICT podniku.
- Umísťování IS do SeGC na základě pravidel určených legislativou (určení konkrétní legislativy podle výsledku výběru právního rámce SeGC).
- Opakované a aktualizované cykly soutěžního mechanismu KeGC.
- Řízení celkové migrace IS do eGC.
- Sledování úspěšnosti budování eGC a migrace do eGC.

Příloha č. 1 *Cíle a měřitelné parametry budování a provozu eGC* popisuje metriky pro sledování dlouhodobé úspěšnosti budování eGC ve Fázi III.

10.2 Plán legislativních změn

V průběhu Fáze II. budou rozpracovány, připraveny a schváleny legislativní změny v následujících oblastech, v souladu s koncepty popsanými v tomto dokumentu.

10.2.1 Legislativní změny nepřímo související s eGC

Informační koncepce ČR, připravovaná na základě **podle §5a (1) ZoISVS a v rámci strategie Digitální Česko** odborem Hlavního architekta MV, a následné metodické materiály, které budou jejím rozpracováním, obsahuje vybudování eGC jako jeden ze svých cílů. Příprava dokumentů Informační koncepce ČR a eGC je koordinována.

„Cloudová vyhláška NÚKIB“ (podle §6 (e) ZoKB) je nový prováděcí předpis, který stanoví "obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu". Vyhláška je připravovaná NÚKIB ve spolupráci s týmem B projektu Příprava vybudování eGC na základě metodiky hodnocení bezpečnostních dopadů eGC. Tato vyhláška má stanovit čtyři bezpečnostní úrovně cloudových služeb na základě hodnocení bezpečnostních dopadů IS, který je používá, a určit pro ně bezpečnostní požadavky/opatření. Pro nejvyšší úroveň má určit, že musí být provozovány v datových centrech a na HW a SW platformách v majetku státu a provozované organizacemi řízenými státem (OSS nebo státní podniky), v rámci provozu musí být ošetřená autorská práva třetích stran (zákaz vendor-locku).

10.2.2 Legislativní změny přímo související s eGC

Legislativní rozpracování variant řešení právního rámce, včetně koncepčního zadání souvisejících změn legislativy, a doporučení jedné z variant bude provedeno meziresortní komisí garantů jednotlivých relevantních zákonů – MV (ZoISVS), MF (ZoRP), MPO (ZoSP) a MMR (ZZVZ) – ve spolupráci s pracovní skupinou RVIS pro přípravu vybudování eGovernment cloudu na základě požadavků, kritérií a variant uvedených v tomto dokumentu (SAZ). Termín předložení legislativního rozboru a doporučené varianty vládě je do 30.6.2019. Koncepční zadání legislativních změn bude podkladem pro úkoly v usnesení vlády pro jednotlivé ministry.

V rámci činnosti této meziresortní komise budou projednány a finalizovány i následující náměty na případné legislativní změny, vyplývající z požadavků formulovaných v tomto dokumentu (SAZ):

Zákon č. 365/2000 Sb., o ISVS, případně Informační koncepce ČR (podřízený právní předpis), garant Ministerstvo vnitra

- status eGC, ŘOeGC a jeho vztah k dalším útvarům řízení ICT VS, …,
- pravidla umísťování do eGC (cloud first, hodnocení bezpečnostní úrovně, umísťování do KeGC a SeGC, kalkulace TCO a odpovídající pravidla účetnictví a rozpočetnictví),
- rozšíření mechanismu stanovisek OHA dle nařízení vlády č. 889/2015 a zákona č. 365/2000 Sb. o posouzení využívání služeb eGC (ve spolupráci s ŘOeGC).

Zákon č. 134/2016 Sb., o zadávání veřejných zakázek, garant Ministerstvo pro místní rozvoj

- podpora soutěžních mechanismů a nástrojů vhodných pro KeGC s využitím vlastností cloud brokeru včetně přímého objednávání služeb na základě konkrétních cenových nabídek předem poskytnutých dodavateli.

Bude upraven formulář RIA (měření dopadů) o zdůvodnění využití nebo nevyužití eGC.

Dále je třeba identifikovat, revidovat a postupně upravit specifické zákony upravující statut jednotlivých OSS a jejich agendových systémů, které mohou formulovat povinnost poskytovat ICT služby pro určité agendy způsobem, který je nekompatibilní s externím nákupem služeb eGC.

11 Seznam zkratek

CENDIS	Centrum dopravních informačních systémů
CMS	Centrální místo služeb
DC	Datové centrum
DCaaS	Data center as a Service
DCeGov	Dohledové centrum eGovernmentu
DNS	Dynamický nákupní systém
DPIA	Data Protection Impact Assessment
eGOV	eGovernment
eGC	eGovernment cloud
eGSB	eGon Service Bus
ESIF	Evropské strukturální a investiční fondy
GDPR	General Data Protection Regulation
HSM	Hardware security module
IaaS	Infrastructure as a service
ICT	Information and communication technologies (informační a komunikační technologie)
IK	Informační koncepce
IS	Informační systém
ISoISVS	Informační systém o ISVS
ISVS	Informační systém veřejné správy
ISZR	Integrovaný systém základních registrů
ITIL	Information Technology Infrastructure Library
JŘBU	Jednací řízení bez uveřejnění
KeGC	Komerční část eGC
KII	Kritická informační infrastruktura
KIVS	Komunikační infrastruktura veřejné správy
MF	Ministerstvo financí

MMR	Ministerstvo pro místní rozvoj
MV	Ministerstvo vnitra
MPO	Ministerstvo průmyslu a obchodu
NAKIT	Národní agentura pro komunikační a informační technologie
NDA	Nondisclosure agreement
NBÚ	Národní bezpečnostní úřad
NEN	Národní elektronický nástroj
NIX	Nezávislá internetová Exchange NIX.CZ
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OHA	Odbor hlavního architekta eGovernmentu MV
OKB	Odbor kybernetické bezpečnosti a koordinace ICT MV
OSS	Organizační složka státu
OVM	Orgán veřejné moci
OVS	Orgán veřejné správy
OVZ	Odbor veřejných zakázek MV
PaaS	Platform as a Service
PAYC	Pay as you consume
RVIS	Rada vlády pro informační společnost
ŘOeGC	Řídící orgán eGC
SaaS	Software as a service
SAZ	Souhrnná analytická zpráva
SDEU	Soudní dvůr EU
SeGC	Státní část eGC
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SPCSS	Státní pokladna Centrum sdílených služeb
TCO	Total Cost of Ownership, celkové náklady životního cyklu

ÚOHS	Úřad pro ochranu hospodářské soutěže
ÚOOÚ	Úřad pro ochranu osobních údajů
VIS	Významný informační systém
VoKB	Vyhláška o kybernetické bezpečnosti (82/2018 Sb.)
VS	Veřejné správa
VZ	Veřejná zakázka
ZoISVS	Zákon o ISVS
ZoKB	Zákon o kybernetické bezpečnosti
ZoOOÚ	Zákon o ochraně osobních údajů
ZoOUI	Zákon o ochraně utajovaných informací
ZoRP	Zákon o rozpočtových pravidlech
ZoSP	Zákon o státním podniku
ZVZ	Zákon o veřejných zakázkách
ZZVZ	Zákon o zadávání veřejných zakázek