



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky



# Příprava vybudování eGov Cloudu (eGC)

Postup prací v pracovních týmech eGC

**Policejní akademie ČR v Praze**  
**22. 6. 2017**

# Obsah

## **1. Stav projektu eGovernment Cloud (eGC) v ČR**

- *Ing. Miroslav Tůma, Ph.D. (MV)*

## **2. Synergie služeb státní části a komerční části eGC. Obsahová a provozní stránka, katalog služeb eGC**

- *Dušan Kučera (SPCSS), Ing. Pavel Hrdlička (OV) a tým provozně/obsahový*

## **3. Bezpečnost v cloudu: Úrovně zabezpečení služeb dle hodnocení dopadů, bezpečnostní opatření založená na standardech, soulad se ZoKB a GDPR**

- *plk. Ing. Tomáš Hampl (PČR) a tým bezpečnost*

## **4. Ekonomické aspekty cloudových služeb**

- *Ing. Michal Pešek (SZR), Martin Dolný (OV), Petr Leština (OV) a tým ekonomika*

## **5. Legislativní zakotvení eGC**

- *Bc. Tomáš Bezouška (ÚV) a tým legislativa*

## **6. Pravidla a procedury eGC**

- *prof. Ing. Jiří Voříšek (VŠE) a tým procesy*



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky



# eGovernment Cloud ČR – Národní Cloud Computing – stav přípravy

**Ing. Miroslav Tůma, Ph.D.**

## **Strategický rámec Národního cloud computingu – eGovernment cloud ČR**

- **Strategický rámec eGC představuje zásadní principy fungování eGovernmentu cloudu (eGC) a potřebné kroky nezbytné k jeho vybudování a využívání v prostředí ČR**
- **Strategický rámec je postaven na následujících předpokladech:**
  - ✓ **státní část eGC**
  - ✓ **komerční část eGC**
  - ✓ eGC v I. fázi poskytuje výpočetní výkon (IaaS) pro IS státní správy (neumísťuje se vlastní HW, ale pouze IS státní správy)
  - ✓ Umisťování aplikací bude ctít principy:
    - Postupná migrace stávajících IS nenásilnou formou
    - Nové / inovované IS musí být umístěny do eGC.
    - IS a data státu, která mají pro stát strategický význam, musí být ve státní části eGC, tj. nemohou být umístěny do komerční části eGC
  - ✓ Existence přesně specifikovaných výjimek a pravidel
- **Schváleno Usnesením vlády č. 1050 ze dne 28. listopadu 2016**

## projekt Příprava vybudování eGovernment cloudu

- **Zpracování komplexních analýz** - na základě kterých dojde k upřesnění a definici základních podmínek realizace eGC (státní a komerční části) pro navazující FÁZI II a III v oblasti legislativní, ekonomické, provozní, bezpečnostní, organizační, které zanalyzují např:
  - ✓ Požadavky na státní a komerční část - provozní, bezpečnostní, SLA, ...
  - ✓ Analýzu IS státu - stanovení strategických IS státu, stanovení úrovně dopadu
  - ✓ Stanovení standardů eGC – platform, služeb, ...
  - ✓ Stanovení jasných a přesně specifikovaných výjimek
  - ✓ Zajištění právní podpory (z.č. 365/2000 Sb., z.č. 134/2016 Sb., ...)
  - ✓ Kalkulace potřebných kapacit státní části
  - ✓ Analýzu datových center státu – současné kapacity
  - ✓ Pravidla financování státní části eGC
  - ✓ Metodiku hodnocení efektivity umístění IS do eGC – TCO
  - ✓ Proces umístění IS do eGC – metodika migrace
- **Výstupy projektu** „Příprava vybudování eGovernment cloudu“ budou předloženy Vládě ČR k rozhodnutí o dalším postupu.

## **Pracovní skupina pro Přípravu vybudování eGC**

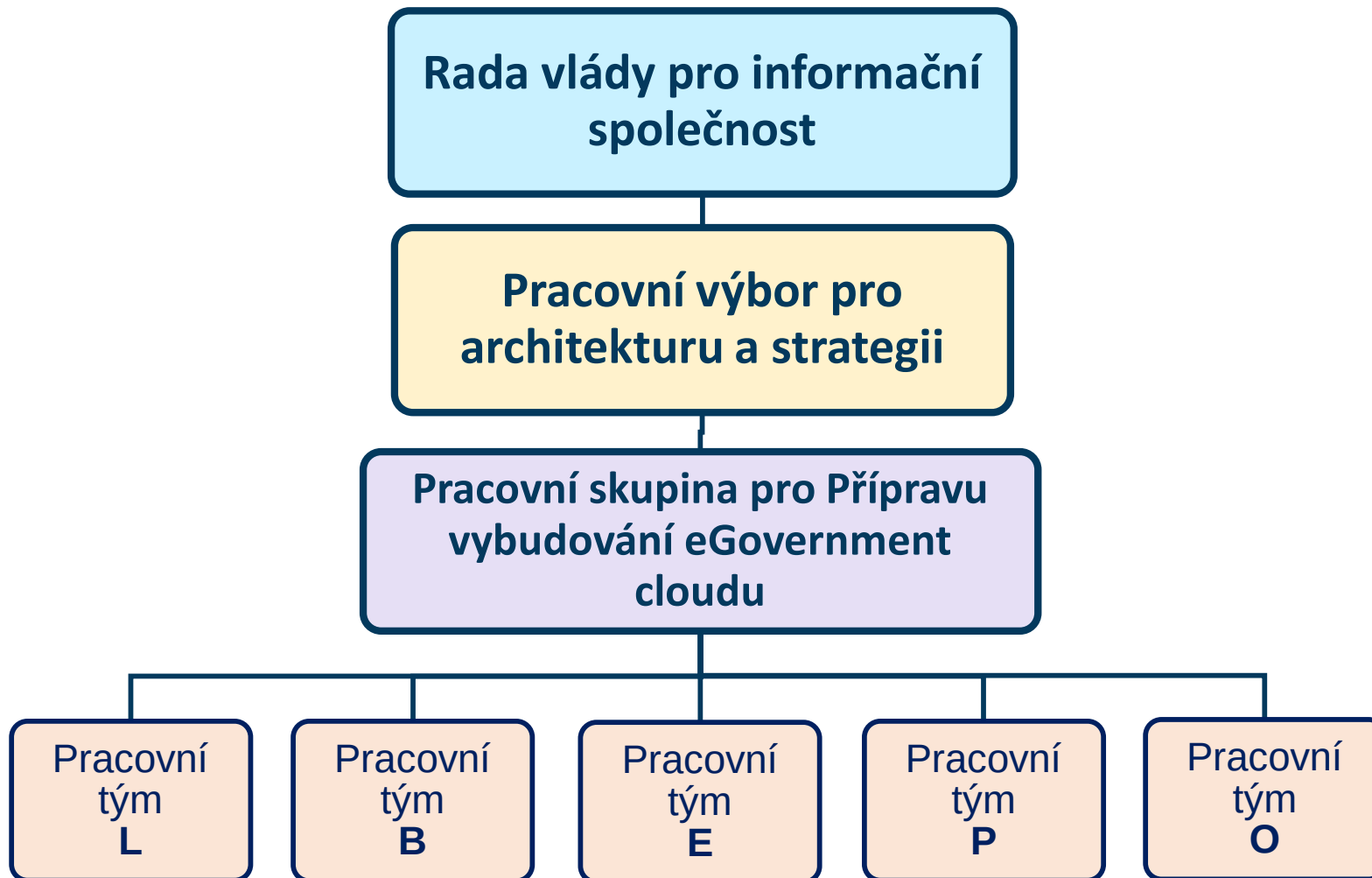
### ➤ **Vznik Pracovní skupiny eGC pod RVIS**

- ✓ Členy pracovní skupiny jsou zástupci jednotlivých resortů, ústředních orgánů státní správy, zpravodajských složek a odborné veřejnosti včetně akademické sféry,
- ✓ Vedoucí Pracovní skupiny eGC: Ing. Miroslav Tůma, Ph.D.
- ✓ Aktuálně nominováno 64 členů.

### ➤ **Činnost Pracovní skupiny eGC – zahájena 16.12. 2016**

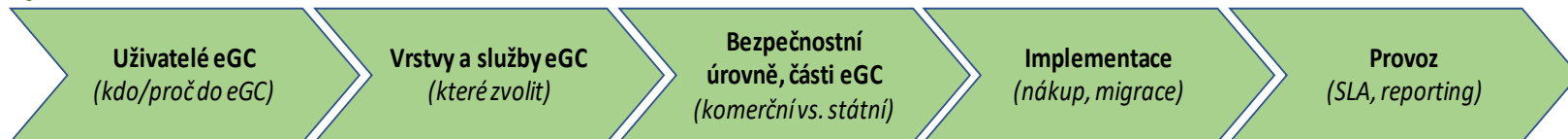
- ✓ Realizace projektu „Příprava vybudování eGovernment cloudu“ a vypracování komplexní analytické zprávy v oblastech:
  - Legislativní/právní (L),
  - Bezpečnostní (B),
  - Ekonomická (E),
  - Provozní/obsahová (P),
  - Organizační/procesní (O),
- ✓ Pracovní týmy se průběžně schází a zpracovávají jednotlivé definované výstupy, které schvaluje Board Pracovní skupiny eGC složený z vedoucích pracovních týmů a dalších odborníků, výstupy jsou postupně zapracovávány do jednotného analytického výstupu.

## Organizace Pracovní skupiny eGC



## Základní struktura problematiky eGC

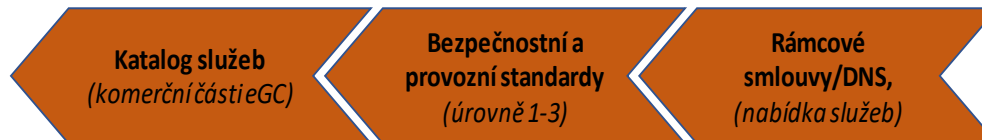
### Správce ISVS



### Řídící orgán eGC



### Provozovatel komerční části eGC



### Provozovatel státní části eGC





## projekt Příprava vybudování eGovernment cloudu

**Termín pro finální zpracování projektu**

**„Příprava vybudování eGovernment cloudu“**

**a jeho předložení vládě k rozhodnutí o dalším postupu**

**4Q 2017**



*... děkuji za pozornost a čas,  
přeji hezký den*

**Ing. Miroslav Tůma, Ph.D.**

ředitel odbor Kybernetické bezpečnosti a koordinace ICT

[miroslav.tuma@mvcv.cz](mailto:miroslav.tuma@mvcv.cz)

GSM: +420 734 267 036



# **Synergie služeb státní části a komerční části eGC. Obsahová a provozní stránka, katalog služeb eGC.**

**Pracovní tým pro provozní/obsahové skupiny**

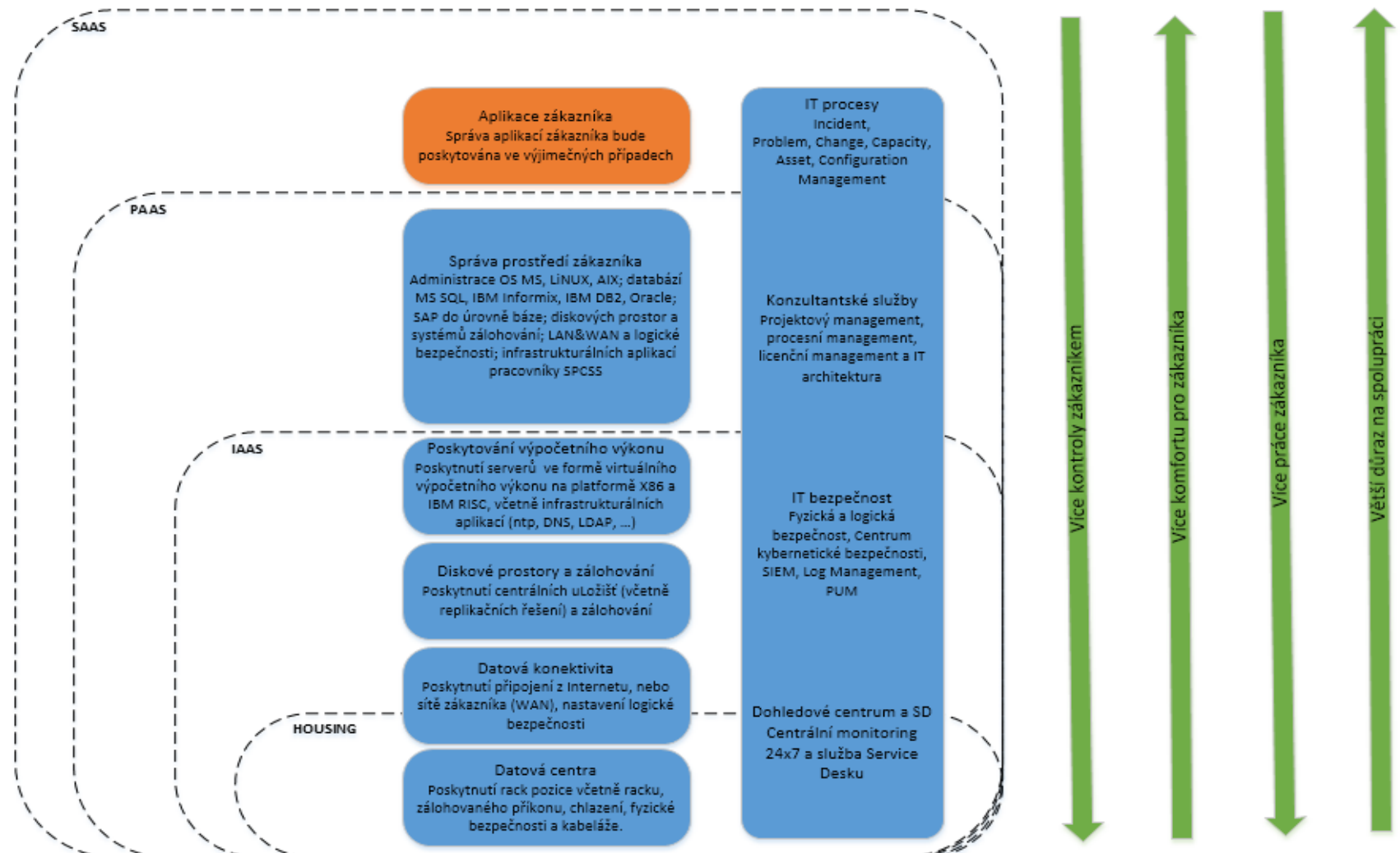
**Dušan Kučera, Ing. Pavel Hrdlička**



## Katalog služeb



## Katalog služeb





## Katalog služeb

| Identifikace SL      | Třída služby                | Jednotka                                 |
|----------------------|-----------------------------|------------------------------------------|
| Housing              | RP v DC Tier III (800x1200) | Rack pozice s včetně racku               |
|                      | RP v DC TIER III (600x1200) |                                          |
|                      | 1kWhpm                      | Příkon v hodnotě 1kW za měsíc            |
|                      | Instalace zařízení          | Jedno zařízení jednorázově               |
| Správa DWDM          | Critical                    | Lambda služba za měsíc                   |
|                      | High                        |                                          |
| Správa Firewall a LB | FW - Box                    | zařízení za měsíc                        |
|                      | FW - Virtual                |                                          |
|                      | LB - Box                    |                                          |
|                      | LB - Virtual                |                                          |
| Správa LAN           | Typ: Low                    | 100Mbps Port za měsíc                    |
|                      | Typ: Middle                 | 1Gbps Port za měsíc                      |
|                      | Typ: High                   | 10Gbps Port za měsíc                     |
| Internet access      | Internet                    | 10 Mbps za měsíc                         |
|                      | Internet                    | 20 Mbps za měsíc                         |
|                      | Internet                    | 30 Mbps za měsíc                         |
|                      | Internet                    | 50 Mbps za měsíc                         |
|                      | Internet                    | 100 Mbps za měsíc                        |
|                      | Internet                    | 500 Mbps za měsíc                        |
|                      | Internet                    | 1000 Mbps za měsíc                       |
|                      | Veřejné IP adresy**         | Plus 16 veřejných IP adres jednorázově   |
|                      | Doplňkové služby 10 Mbps*   | Web proxy a filtr obsahu Služba za měsíc |
|                      |                             | E-mail Antivir/Antispam Služba za měsíc  |
|                      | Doplňkové služby 20 Mbps*   | Web proxy a filtr obsahu Služba za měsíc |
|                      |                             | E-mail Antivir/Antispam Služba za měsíc  |
|                      | Doplňkové služby 30 Mbps*   | Web proxy a filtr obsahu Služba za měsíc |
|                      |                             | E-mail Antivir/Antispam Služba za měsíc  |
|                      | Doplňkové služby 50 Mbps*   | Web proxy a filtr obsahu Služba za měsíc |
|                      |                             | E-mail Antivir/Antispam Služba za měsíc  |
| VPN gateway          | VPN Gateway                 | 1 concurrent user za měsíc               |



## Katalog služeb

| Identifikace SL                                 | Třída služby                                                   | Jednotka                             |
|-------------------------------------------------|----------------------------------------------------------------|--------------------------------------|
| Zálohování a archivace dat                      | Místní záloha                                                  | GB protečený přes backup server      |
|                                                 | Vzdálená záloha                                                |                                      |
| Poskytování diskového prostoru                  | Block Storage - Produktivní pole (Stor1)                       | GB za měsíc                          |
|                                                 | Block Storage - Sekundární pole (Stor 2)                       |                                      |
|                                                 | Block Storage - Backup pole (Back)                             |                                      |
|                                                 | File Storage                                                   |                                      |
|                                                 | Object Storage                                                 |                                      |
|                                                 | Mass Storage                                                   |                                      |
| Poskytování výpočetního výkonu (HW)             | x86 – plán A                                                   | 1 VCPU + 4 GB VRAM za měsíc          |
|                                                 | x86 – plán B                                                   | 1 VCPU + 2 GB VRAM za měsíc          |
|                                                 | RISC                                                           | 0,1 VCPU + 1,77 GB VRAM za měsíc     |
| User management (IAM+PIM)                       | Critical                                                       | Služba (za spravovaný účet) za měsíc |
| Poskytování služby ServiceDesk                  | Service Desk                                                   | SPoC za měsíc                        |
|                                                 | Service Desk                                                   | 1 kontakt / ticket za měsíc          |
| Poskytování monitoringu infrastruktury a služeb | Monitorovací systém Business                                   | PMS za měsíc                         |
|                                                 | Zákaznický portál - Business                                   | PZP za měsíc                         |
|                                                 | Zřízení/změna/ukončení monitoringu aplikace infrastruktury a s | Aplikace/služba jednorázově          |



## Katalog služeb

| Identifikace SL            | Třída služby                   | Jednotka                                   |
|----------------------------|--------------------------------|--------------------------------------------|
| Správa databáze            | Oracle RAC                     | Databázová instance <sup>za měsíc</sup>    |
|                            | Oracle/DB2/Informix            |                                            |
|                            | MS SQL Cluster                 |                                            |
|                            | MS SQL                         |                                            |
|                            | MySQL/PostgreSQL               |                                            |
|                            | Cluster DB startup/rundown     | Databázová instance <sup>jednorázově</sup> |
|                            | DB startup/rundown             |                                            |
| Správa operačních systémů  | Microsoft/Unix/Linux           | Instance OS <sup>za měsíc</sup>            |
|                            | Server startup/rundown         | server <sup>jednorázově</sup>              |
| Správa e-mailových služeb  | Mail systém                    | Mailbox <sup>za měsíc</sup>                |
|                            | Antivir/Antispam               | Mailbox <sup>za měsíc</sup>                |
|                            | Mail system startup/rundown    | Mail system <sup>jednorázově</sup>         |
| Správa aplikačních serverů | Doplňková služba loadbalancing | Instance apl. serveru <sup>za měsíc</sup>  |
|                            | MS IIS/Apache/J2EE/WS          |                                            |
|                            | System startup/rundown         |                                            |
| Poskytování služby SOC     | SIEM Basic                     | PVU <sup>za měsíc</sup>                    |
|                            | System startup/rundown         | PVU za <sup>měsíc</sup>                    |

## Katalog služeb

- Vytvořen pracovní návrh katalogového listu pouze jako „demo“.
- Musí být změněn/dopracován v rámci konkrétních požadavků ostatních pracovních skupin / předmětných rozhodnutí řídící pracovní skupiny.
- Prozatím implementován pouze požadavek Bezpečnostní skupiny
- Musí být zohledněny ty parametry, které budou sloužit k automatizaci procesů v rámci úrovně služeb úrovně automatizace – „Orchestration“ a „Brokerage“
  - Proces výběrového řízení
  - Proces odsouhlasení transakcí
  - Zveřejnění informací
  - Relace na jiné služby katalogu
  - Bezpečnostní zařazení
  - Ekonomické/Finanční parametry
  - Technické parametry pro virtualizační vrstvy

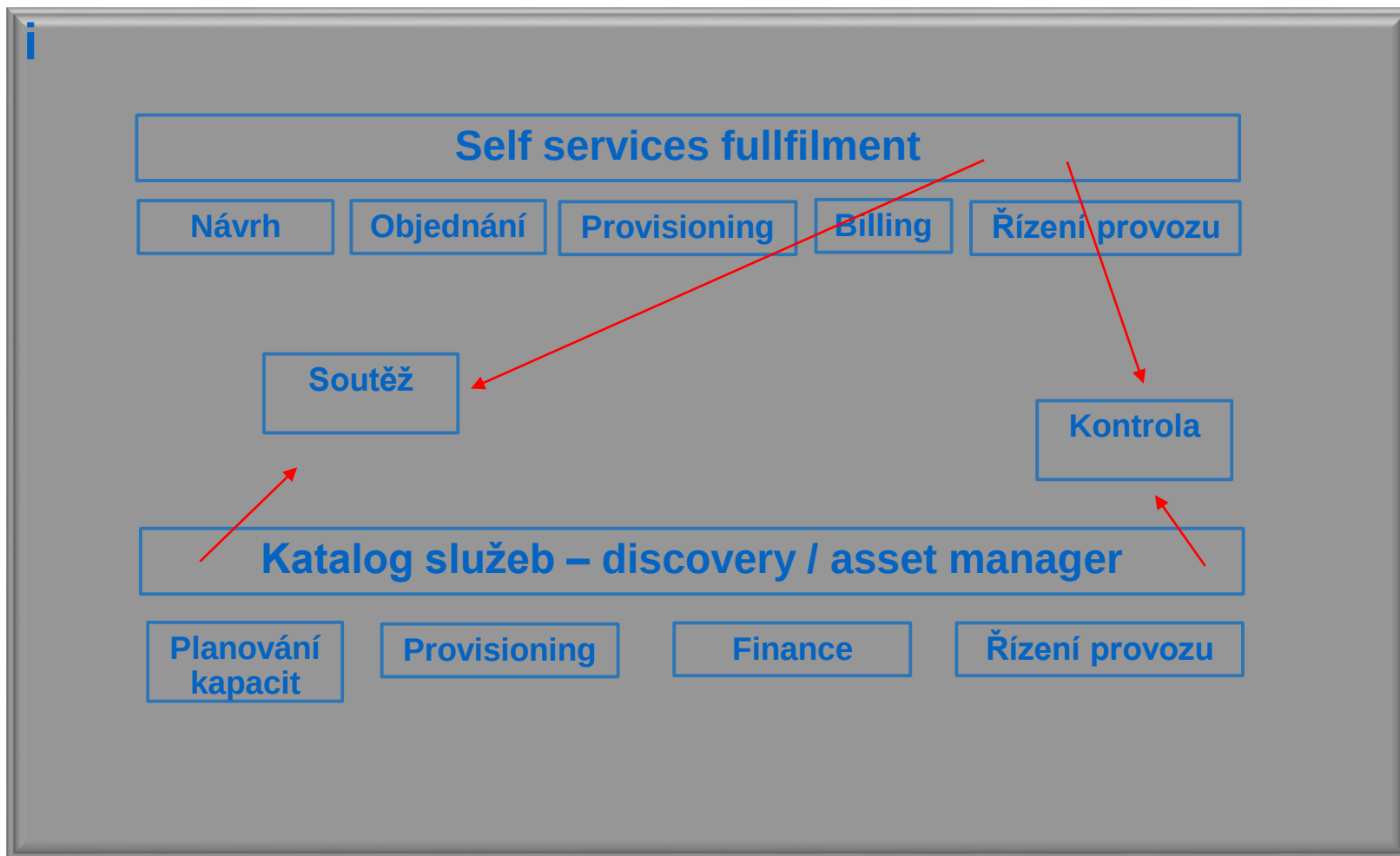
## Hybridní cloud

Na rozdíl od konceptu virtualizace (byť v datových centrech), je koncept cloudu podstatně robustnější. Cloudové služby poskytované zákazníkovi/klientovi jsou typicky realizovány v prostředí s vysoce pokročilou orchestrací a managementem, vysokým stupněm bezpečnosti a ochrany soukromí klienta a řadou dalších služeb.

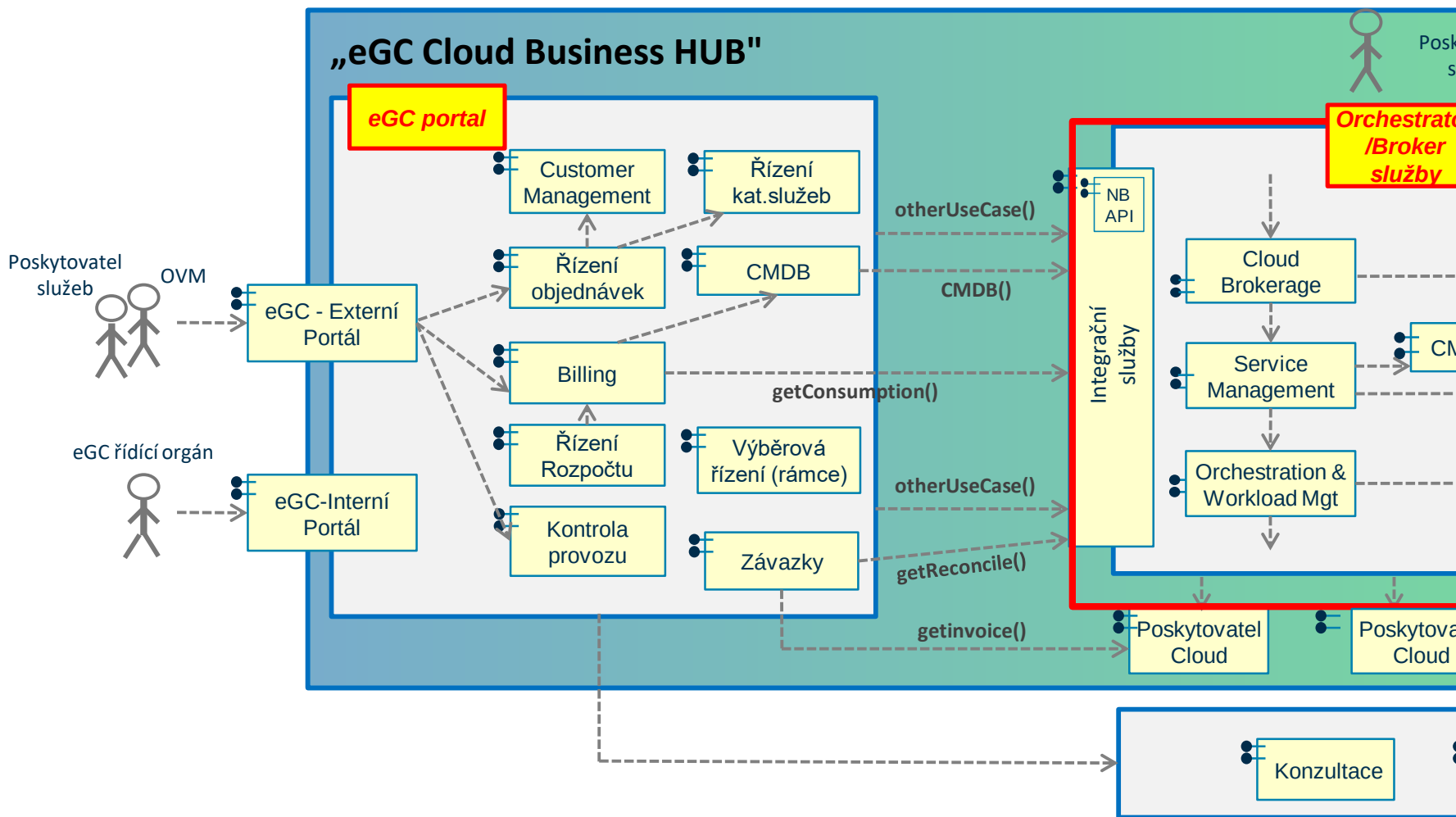
Obecně lze říci, že cloudová řešení lze rozdělit na:

- privátní cloud, tedy řešení tzv. „on premise“, kde cloud technologie jsou umístěny v prostorech subjektu a jsou pracovníky tohoto subjektu přímo spravovány.
- státní cloud, tedy obdoba komunitního cloudu, kdy cloudové řešení provozuje pro organizace státní správy případně v prostředí veřejné správy pro podřízené krajské organizace vybraný subjekt státem nebo krajem přímo kontrolovaný či vlastněný nebo subjekt pro tyto účely vybraný ve veřejné soutěži
- komerční cloud, tedy řešení, kdy informace a informační systémy jsou umístěny v komerčně provozovaných řešeních
- Hybridní cloud je kombinací privátního cloudu a komerčního cloudu, případně kombinací privátního a státního cloudu, kdy dochází k technologicky nebo ekonomicky výhodnému propojení více infrastruktur, platforem nebo aplikací. Dochází tak zpravidla k rozdělení provozu a správy mezi více subjektů, kdy v části privátního cloudu nebo státního cloudu mohou být umístěna aktiva, která nechce daný subjekt z jakéhokoliv důvodu umístit do komerčního cloudu, zatímco jiná aktiva nebo služby mohou být provozovány v komerčním cloudu.

## Hybridní Cloud - Cloud Broker / orchestrator



## Hybridní Cloud - Cloud Broker / orchestrator





*... děkujeme za pozornost a čas,  
přejeme hezký den*

**Dušan Kučera, Ing. Pavel Hrdlička**

Dusan.Kucera@spcss.cz

Pavel.Hrdlicka@cz.ibm.com

# **Bezpečnost v eGC: Úrovně zabezpečení služeb dle hodnocení dopadů, bezpečnostní opatření založená na standardech, soulad se ZoKB a GDPR**

**Bezpečnostní tým  
plk. Ing. Tomáš Hampel  
Mgr. Vladimír Rohel  
Ing. Zdeněk Jiříček**

## **Pracovní tým Bezpečnost**

### ➤ **Zástupci**

- Státní organizace
- „Bezpečnostní složky“
- NBÚ / NCKB
- ÚOOÚ
- Státní podniky (NAKIT, SPCSS)
- Odborná veřejnost (společná nominace Hospodářské komory, Svazu průmyslu, ICT Unie, AFCEA)

### ➤ **Poslání**

- Pravidla umístění do státní nebo komerční části eGC - Bezpečnost
  - Viz Strategický rámec eGC: rozpracovat bezpečnostní kritéria, kdy je nutné umístění do státní části eGC, a kdy lze využít komerční cloudové služby
- Stanovení bezpečnostních požadavků na obě části SeGC, KeGC

## Pravidla pro umíst'ování aplikací a dat do eGC

- Umístění do státní nebo komerční části eGC dle **hodnocení úrovní dopadů** ISVS nebo dekomponovaných ICT služeb
- Výjimky z přechodu do eGC (zůstává on-premise)
  - **Bezpečnostní sbory a zpravodajské služby:** výjimka z přechodu do eGC, pokud provoz těchto systémů souvisí s plněním zákonem jim stanovených úkolů. O výjimce z uvedeného může rozhodnout příslušný bezpečnostní sbor/zpravodajská služba.
  - **Oblasti národní bezpečnosti:** obdoba definice U.S. "[National Security Systems](#)". Mohou zpracovávat utajované, avšak i neutajované informace.
- Samospráva: dobrovolně, na základě publikované metodiky a výhodnosti

## Východiska pro úrovně dopadů

- Aplikují se na celé ISVS nebo dekomponované ICT služby eGC
- Posuzování dopadů v 9 vybraných oblastech
  - Bezpečnost a zdraví osob, Ochrana osobních údajů, Důvěryhodnost OVM
  - Povinnosti ze zákona, Řízení a provoz OVM, Mezinárodní vztahy
  - Veřejný pořádek, Trestně-právní jednání, Finanční ztráty
- 4 úrovně dopadů, způsobené:
  - Nedostupnost systému nebo dat
  - Únik a možné zneužití dat (ztráta důvěrnosti)
  - Ztráta dat (od doby zálohy, úplná ztráta)
  - Integrita dat (neúmyslná; úmyslná; syst. chyba)
- „Kalibrace“ úrovní dopadu:
  - KII(ZKB) mapuje svými průřezovými kritérii do úrovně eGC „Kritická“

| Úroveň dopadů | Státní část                                         | Komerční část |
|---------------|-----------------------------------------------------|---------------|
| Nízká         | Pouze v rámci vertikální spolupráce OVM, a mimo eGC | Ano           |
| Střední       |                                                     | Ano           |
| Vysoká        |                                                     | Ano           |
| Kritická      | Ano                                                 | Ne            |

## Tabulka úrovní dopadů

| Úroveň dopadu |          | Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) |                                                                                                                                           |                                                                                                         |                                                                                                                                           |                                                                                                                     |                                                                                                                                         |                                                                                                                                                                      |                                                                                                                                                                                                       |                                                                                   |
|---------------|----------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
|               |          | A. Bezpečnost a zdraví osob                                                                                        | B. Ochrana osobních údajů                                                                                                                 | C. Povinnosti ze zákona                                                                                 | D. Trestně-právní jednání                                                                                                                 | E. Veřejný pořádek                                                                                                  | F. Mezinárodní vztahy                                                                                                                   | G. Řízení a provoz OVM                                                                                                                                               | H. Ztráta důvěryhodnosti                                                                                                                                                                              | I. Finanční ztráty                                                                |
| 1             | nízká    | žádné vodítko                                                                                                      | Porušení etických nikoli však zákonných nebo podzákonných norem vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.    | Správný, občanskoprávní nebo smírčí řízení vedoucí k pokutě nebo k náhradě škody ve výši do 500 tis. Kč | žádné vodítko                                                                                                                             | žádné vodítko                                                                                                       | žádné vodítko                                                                                                                           | Naruší řádné řízení nebo fungování části nebo celé státní organizace.                                                                                                | Negativně ovlivní vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.            | Přímo nebo nepřímo povede ke ztrátám menším než 0,05% ročního rozpočtu OSS / OVM. |
| 2             | střední  | Pravděpodobně povede k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.          | Porušení zákonných nebo podzákonných norem vedoucí k negativním osobním dopadům na jednotlivce.                                           | Správný, občanskoprávní nebo smírčí řízení vedoucí k pokutě nebo k náhradě škody ve výši 0,5-5 mil. Kč  | Může vytvořit podmínky pro páchaní trestné činnosti nebo může ztížit její vyšetřování.                                                    | Pravděpodobně zapříčiní rozsahem, formou nebo místem omezené protesty.                                              | Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.                                                              | Bude bránit v provádění důležitých činností státní organizace.                                                                                                       | Negativně ovlivní vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká avšak krátkodobá.                                      | Přímo nebo nepřímo povede ke ztrátám mezi 0,05% a 1% ročního rozpočtu OSS / OVM.  |
| 3             | vysoká   | Pravděpodobně povede k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob.                | Porušení zákonných nebo podzákonných norem vedoucí k negativním dopadům na velkou skupinu osob. Správní pokuty až do výše 20.000.000 EUR. | Správný, občanskoprávní nebo smírčí řízení vedoucí k pokutě nebo k náhradě škody přesahující 5 mil. Kč  | Napomůže spáchání trestného činu se sazbou do 5 let (např. úmyslný trestný čin) nebo znemožní vyšetřování takového trestného činu.        | Pravděpodobně způsobí veřejné nepokoje, které mohou mít i celostátní důsledky.                                      | Může vytvářet negativní obraz ČR ve světě.                                                                                              | Závažným způsobem poškozuje účinný rozvoj nebo prosazení státní politiky nebo může způsobit zastavení nebo podstatné narušení základních činností státní organizace. | Závažně ovlivní vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.                                                                                              | Přímo nebo nepřímo povede ke ztrátám mezi 1% a 10% ročního rozpočtu OSS / OVM.    |
| 4             | kritická | Může vést k ohrožení života jedné nebo několika osob.                                                              | žádné vodítko                                                                                                                             | žádné vodítko                                                                                           | Napomůže spáchání trestného činu se sazbou od 5 let (např. zvlášť závažný trestný čin) nebo znemožní vyšetřování takového trestného činu. | Způsobí hromadné nepokoje, např. generální stávku, nebo jinak závažně naruší veřejný pořádek s celostátními dopady. | Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR. (v případě důvěrnosti stupeň Vyhrazené) | Závažným způsobem zasáhne do fungování státu jako celku, zemožňuje řízení státních institucí a výkon veřejné správy                                                  | Závažně a dlouhodobě ovlivní vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti. | Přímo nebo nepřímo povede ke ztrátám přesahujícím 10% ročního rozpočtu OSS / OVM. |

## Kontext bezp. opatření vůči stávající legislativě

### ➤ Vymezení vůči zákonu č. 412/2005 Sb.

- „**Kritická** úroveň dopadů“ v oblasti „Důvěrnost“ odpovídá nejvýše stupni utajení „**Vyhrazené**“ (za jistých okolností – pouze služby státní části eGC).

### ➤ Vymezení vůči zákonu č. 181/2014 Sb.

- Jestliže je v některé z oblastí dopadů dosaženo úrovně „Vysoká“, popř. „Kritická“ může správce zvážit zařazení IS mezi významné informační systémy (**VIS**).
- Průřezová kritéria pro určení prvku **KI** dle §1 nařízení vlády č. 432/2010 Sb. budou ve většině případů odpovídat hodnocení dopadů v úrovni „**kritická**“ dle této metodiky.

### ➤ Vymezení vůči Obecnému nařízení GDPR

- Požadavky na zpracování osobních údajů v cloudových službách musí dle nařízení GDPR vycházet z hodnocení rizik daného scénáře zpracování pro práva a svobody fyzických osob.
- V případě zjištění vysokého rizika budou správci povinni provést tzv. „posouzení vlivu zpracování dat na ochranu osobních údajů“ (DPIA, viz čl. 35), a zajistit adekvátní bezpečnostní opatření a mechanismy ochrany.
- Předpokládáme využití některého ze schválených „kodexů chování“ (viz čl. 40) daným zpracovatelem a jeho cloudovou službou. Dozorový úřad (ÚOOÚ) očekává, že do doby účinnosti nařízení GDPR bude schváleno několik kodexů chování, které vytvoří vhodný rámec standardizace.

## Metodika zařazení – konzultace fy. RAC s.r.o.

| Hodnocení narušení bezpečnosti dat a informací na základě interview s respondenty |                                                                                                                                                                                                                                                   | Dostupnost           |                 |                 |                 |                      |                   |                    |                      |                     |                           | Ztráta                       |                              |                              |                               |                               |                  | Důvěrnost                     |                               |                           | Integrita                     |                                |                    |               |   |          |
|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|-----------------|-----------------|-----------------|----------------------|-------------------|--------------------|----------------------|---------------------|---------------------------|------------------------------|------------------------------|------------------------------|-------------------------------|-------------------------------|------------------|-------------------------------|-------------------------------|---------------------------|-------------------------------|--------------------------------|--------------------|---------------|---|----------|
| Respondent                                                                        | Kategorie dat a informací (agenda)                                                                                                                                                                                                                | Nedostupnost 15 min. | Nedostupnost 1h | Nedostupnost 4h | Nedostupnost 8h | Nedostupnost 16 hod. | Nedostupnost 1den | Nedostupnost 2 dny | Nedostupnost 1 týden | Nedostupnost 14 dní | Nedostupnost měsíc a více | Ztráta dat od zálohy (1hod.) | Ztráta dat od zálohy (4hod.) | Ztráta dat od zálohy (8hod.) | Ztráta dat od zálohy (16hod.) | Ztráta dat od zálohy (24hod.) | Úplná ztráta dat | Prozrazení v rámci organizace | Prozrazení smluvním partnerům | Prozrazení vně organizaci | Modifikace dat malého rozsahu | Modifikace dat velkého rozsahu | Úmyslná modifikace |               |   |          |
| doplnit jméno respondenta                                                         | doplnit název AIS / kategorie dat a informací                                                                                                                                                                                                     |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               |   |          |
|                                                                                   | Bezpečnost a zdraví osob                                                                                                                                                                                                                          |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           | 1                            | 1                            | 1                            | 1                             | 1                             | 2                |                               |                               | 3                         | 1                             | 3                              | 4                  | Úroveň dopadu |   |          |
|                                                                                   | Ochrana osobních údajů                                                                                                                                                                                                                            |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               | 1                |                               | 2                             | 3                         |                               | 1                              | 2                  |               | 1 | nízká    |
|                                                                                   | Povinnosti ze zákona                                                                                                                                                                                                                              |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               | 2 | střední  |
|                                                                                   | Trestně-právní jednání                                                                                                                                                                                                                            |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               | 3 | vysoká   |
|                                                                                   | Veřejný pořádek                                                                                                                                                                                                                                   |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               | 4 | kritická |
|                                                                                   | Mezinárodní vztahy                                                                                                                                                                                                                                |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               |   |          |
|                                                                                   | Řízení a provoz OVM                                                                                                                                                                                                                               |                      |                 | 1               | 1               | 1                    | 1                 | 1                  | 2                    | 2                   | 2                         |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               |   |          |
|                                                                                   | Ztráta důvěryhodnosti                                                                                                                                                                                                                             |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               | 1                | 1                             |                               |                           |                               | 1                              | 2                  |               |   |          |
|                                                                                   | Finanční ztráty                                                                                                                                                                                                                                   |                      |                 |                 |                 |                      |                   |                    |                      | 1                   | 1                         |                              |                              |                              | 1                             | 1                             | 1                | 3                             |                               | 2                         | 3                             |                                | 1                  | 2             |   |          |
|                                                                                   |                                                                                                                                                                                                                                                   |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               |   |          |
|                                                                                   | Komentář k dopadům (uveďte odůvodnění k následkům narušení dostupnosti-odkdy a proč začíná mít endostupnost negativní dopad, narušení důvěrnosti-např. porušení zákona č. 101/2000, narušení integrity dat-např. chyba při zpracování dat agendy) |                      |                 |                 |                 |                      |                   |                    |                      |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                               |                                |                    |               |   |          |



## Vodítka pro zařazení ICT služby do úrovně dopadů

| Stanovení požadavků na bezpečnost | základní požadavky na SLA cloudové služby |                                                                                                                                                                                                                                                                                                                                                                                      |                        |              | Dopady narušení dostupnosti |                 |                 |                 |                      |                    |                    |                                                                                                                                                                                                                                                                                       | Ztráta dat          |                           |                              |                              | Úrovně důvěrnosti            |                               |                               | Úrovně integrity |                               |                               |                           |                              |                                                          |                                                                                                                                                          |                                                                                                          |                                                          |                                                            |                                                             |  |  |
|-----------------------------------|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|--------------|-----------------------------|-----------------|-----------------|-----------------|----------------------|--------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|---------------------------|------------------------------|------------------------------|------------------------------|-------------------------------|-------------------------------|------------------|-------------------------------|-------------------------------|---------------------------|------------------------------|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------|-------------------------------------------------------------|--|--|
|                                   | dostupnost                                | úroveň redundance                                                                                                                                                                                                                                                                                                                                                                    | přípustná doba výpadku |              | Nedostupnost 15 min.        | Nedostupnost 1h | Nedostupnost 4h | Nedostupnost 8h | Nedostupnost 16 hod. | Nedostupnost 1 den | Nedostupnost 2 dny | Nedostupnost 1 týden                                                                                                                                                                                                                                                                  | Nedostupnost 14 dní | Nedostupnost měsíc a více | Ztráta dat od zálohy (1hod.) | Ztráta dat od zálohy (4hod.) | Ztráta dat od zálohy (8hod.) | Ztráta dat od zálohy (16hod.) | Ztráta dat od zálohy (24hod.) | Úplná ztráta dat | Prozrazení v rámci organizace | Prozrazení smluvním partnerům | Prozrazení vně organizaci | Neúmyslná modifikace (chyba) | Systémová chyba                                          | Úmyslná modifikace                                                                                                                                       |                                                                                                          |                                                          |                                                            |                                                             |  |  |
|                                   |                                           |                                                                                                                                                                                                                                                                                                                                                                                      | jedinečný              | kumulovaný   |                             |                 |                 |                 |                      |                    |                    |                                                                                                                                                                                                                                                                                       |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                              |                                                          |                                                                                                                                                          |                                                                                                          |                                                          |                                                            |                                                             |  |  |
| nízká                             | 99,0%                                     | Podpora a servis pouze v pracovní dny a ve stanovené pracovní době. Smluvní penále při výpadku dostupnosti delší než jednotlivě 48 hod. (nezapočítávají se dny pracovního volna a dny pracovního klidu) nebo celkem 3,65 dní za rok (odpovídá 99,0%)                                                                                                                                 | do 48 hod.             | do 87,6 hod. | 1                           |                 |                 |                 | 2                    | 2                  | 2                  | Pro časové intervaly, kde se dopady mění z hodnoty 1 na 2, popř. z hodnoty dopadu 2 na 3 je doporučeno vyjasnit výši nákladů, které mají OVM s dodatečnou rekonstrukcí dat z jiných zdrojů (např. papírové formuláře) oproti nákladům spojeným s vyšší frekvencí vytváření záloh dat. |                     |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           | 1                            | 1<br>Nízké požadavky na důvěrnost dat dle matice dopadů. |                                                                                                                                                          |                                                                                                          | 1<br>Nízké požadavky na integritu dat dle matice dopadů. |                                                            |                                                             |  |  |
| střední                           | 99,8%                                     | Smluvní penále při výpadku dostupnosti služby delší než celkem 16 hodin za rok (odpovídá 99,8% s vyhodnocením na roční bázi), a dále v případě jednotlivých výpadků delších než 4 hodiny.                                                                                                                                                                                            | do 4 hod.              | do 16 hod.   | 1                           | 2               | 2               | 2               | 3                    | 3                  | 3                  | 3                                                                                                                                                                                                                                                                                     | 2                   |                           |                              |                              |                              |                               |                               |                  |                               |                               |                           |                              | 2                                                        | 2<br>Střední požadavky na důvěrnost dat dle matice dopadů. V případech, kdy je vyžadována ochrana právními předpisy je nutné zvážit úroveň eGC "vysoká". |                                                                                                          |                                                          | 2<br>Střední požadavky na integritu dat dle matice dopadů. |                                                             |  |  |
| vysoká                            | 99,9%                                     | Fault-tolerantní systém s geo-redundantním uložením dat. Smluvní penále při výpadku dostupnosti služby delším než celkem 8,64 hodin za rok, nebo delším než celkem 43 minut měsíčně. SLA zahrnuje vyhodnocení dostupnosti na měsíční bázi (43 minut odpovídá 99,9% na měsíční bázi), tzn. jakýkoli jeden nebo celkový kumulovaný výpadek delší než 43 minut za měsíc je penalizován. | do 43 min.             | do 8,64 hod. | 1                           | 3               | 3               | 3               | 3                    | 3                  | 4                  | 4                                                                                                                                                                                                                                                                                     | 4                   | 3                         |                              |                              |                              |                               |                               |                  |                               |                               |                           |                              |                                                          | 3                                                                                                                                                        | 3<br>Vysoké požadavky na důvěrnost dat dle matice dopadů, popř. je ochrana vyžadována právními předpisy. |                                                          |                                                            | 3<br>Vysoké požadavky na integritu dat dle matice dopadů.   |  |  |
| kritická                          | 99,99%                                    | Plně fault-tolerantní systém s geo-redundancí a replikací transakčních dat. Smluvní penále při výpadku dostupnosti služby delší než celkem 52 minut za rok (odpovídá 99,99%). Cloudové služby v této úrovni dopadu budou mít smluvně dané max. doby RPO / RTO.                                                                                                                       | do 15 min.             | do 52min.    | 1-2                         | 3-4             |                 |                 |                      |                    |                    |                                                                                                                                                                                                                                                                                       |                     | 4                         |                              |                              |                              |                               |                               |                  |                               |                               |                           |                              |                                                          | 4                                                                                                                                                        | 4<br>Kritické požadavky na důvěrnost dat dle matice dopadů.                                              |                                                          |                                                            | 4<br>Kritické požadavky na integritu dat dle matice dopadů. |  |  |

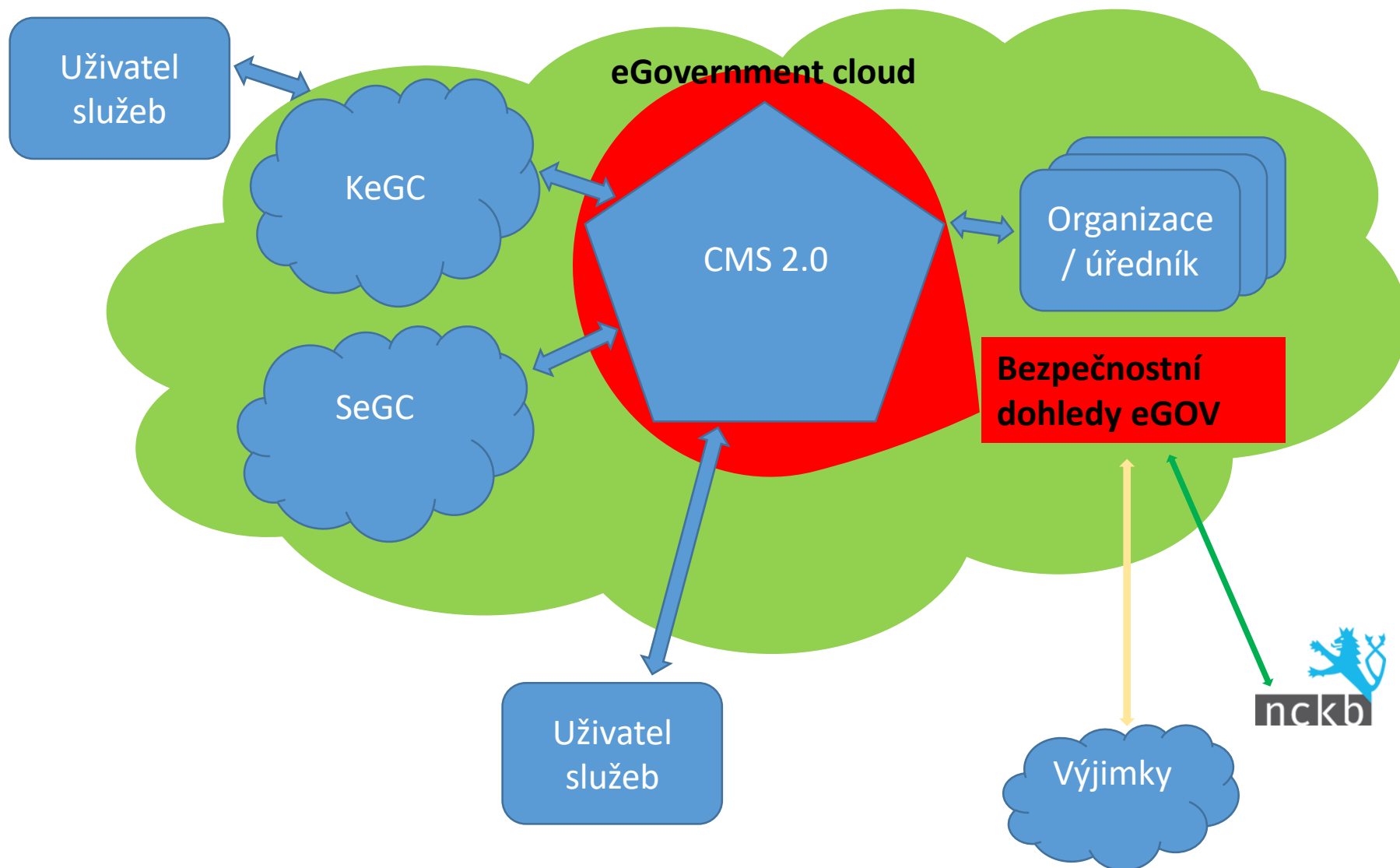


# Bezpečnostní opatření založená na průmyslových standardech (návrh)

## Soubor bezpečnostních opatření (návrh)

| popis opatření                                                                                                                                                                                                                                                | kategorie                    | regulace            | norma                                                   | Níz      | Stř      | Vys      | Kri      | KII      | VIS      | ISVS     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|---------------------|---------------------------------------------------------|----------|----------|----------|----------|----------|----------|----------|
| Smluvní podmínky, které vyplývají z novely ZoKB                                                                                                                                                                                                               | smluvní vztahy               | ZoKB                | Vyhláška č. 316/2014 Sb. §7                             |          |          |          |          | X        | X        |          |
| Smluvní podmínky, které vyplývají z novely zák. o ISVS                                                                                                                                                                                                        | smluvní vztahy               | ZoISVS              | ZoISVS §5b novely                                       |          |          |          |          |          |          | X        |
| Smluvní podmínky, které obsahují závazek účinného zavedení bezp. opatření                                                                                                                                                                                     | smluvní vztahy               | bezpečnost eGC      | ISO 27001 A.15                                          | X        | X        | X        | X        | X        | X        | X        |
| <b>Smluvní podm. dle čl. 28 nařízení GDPR (v případě zpracování osobních údajů)</b>                                                                                                                                                                           | <b>smluvní vztahy</b>        | <b>GDPR</b>         | <b>GDPR, čl. 28</b>                                     | <b>X</b> | <b>X</b> | <b>X</b> | <b>X</b> | <b>X</b> | <b>X</b> | <b>X</b> |
| SLA s garantovanou dostupností dle úrovně dopadů, pod penalizací                                                                                                                                                                                              | smluvní vztahy               | bezpečnost eGC      | ISO 27001 A.15                                          | X        | X        | X        | X        | X        | X        | X        |
| SLA - dostupnost 99 % (dle definice v tabulce úrovně dopadů)                                                                                                                                                                                                  | smluvní vztahy               | bezpečnost eGC      | ISO 27001 A.15.2                                        | X        |          |          |          |          |          |          |
| SLA - dostupnost 99,8 % (dle definice v tabulce úrovně dopadů)                                                                                                                                                                                                | smluvní vztahy               | bezpečnost eGC      | ISO 27001 A.15.2                                        |          | X        |          |          |          |          |          |
| SLA - dostupnost 99,9 % (dle definice v tabulce úrovně dopadů)                                                                                                                                                                                                | smluvní vztahy               | bezpečnost eGC      | ISO 27001 A.15.2                                        |          |          | X        |          |          |          |          |
| SLA - dostupnost 99,99 % (dle definice v tabulce úrovně dopadů)                                                                                                                                                                                               | smluvní vztahy               | bezpečnost eGC      | ISO 27001 A.15.2                                        |          |          |          | X        |          |          |          |
| Self-Assessment dodavatele základní množiny bezp. opatření                                                                                                                                                                                                    | bezpečnostní opatření        | bezpečnost eGC      | ISO 27001 A.15                                          | X        |          |          |          |          |          | X        |
| Certifikace ISO 27001 v širším rozsahu opatření SoA (prohlášení o aplikovatelnosti)                                                                                                                                                                           | bezpečnostní opatření        | bezpečnost eGC/ZoKB | Vyhláška č. 316/2014 Sb. §29                            |          | X        |          |          |          |          |          |
| Certifikace ISO 27001 v plném rozsahu opatření SoA                                                                                                                                                                                                            | bezpečnostní opatření        | ZoKB                | Vyhláška č. 316/2014 Sb. §29                            |          |          | X        | X        | X        | X        |          |
| Certifikace ISO 27017                                                                                                                                                                                                                                         | bezpečnostní opatření        | bezpečnost eGC/ZoKB |                                                         |          |          | X        | X        | X        | X        |          |
| <b>Certifikace ISO 27018 (v případě zpracování osobních údajů)</b>                                                                                                                                                                                            | <b>bezpečnostní opatření</b> | <b>GDPR</b>         | <b>GDPR, čl. 32</b>                                     |          |          | <b>X</b> | <b>X</b> |          |          |          |
| <b>Deklarace dodržování některého ze schválených kodexů chování dle scénáře zpracování</b>                                                                                                                                                                    | <b>bezpečnostní opatření</b> | <b>GDPR</b>         | <b>Budoucí prováděcí předpisy k GDPR</b>                |          |          |          |          |          |          |          |
| Deklarace místa uložení dat a způsob ošetření souvisejících rizik                                                                                                                                                                                             | bezpečnostní opatření        | bezpečnost eGC      | ISO 27001 A.9, A.11                                     |          | X        | X        | X        | X        | X        | X        |
| Požadavky BC/DR a georedundanci dat                                                                                                                                                                                                                           | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.17, Vyhláška č. 316/2014 Sb. §14            |          |          | X        | X        | X        |          |          |
| Ochrana dat šifrováním v úložištích, nástroje pro kontrolu klíčů povinnou osobou                                                                                                                                                                              | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.10                                          |          |          | X        | X        | X        |          |          |
| Nástroje RBAC a 2-factor authN pro všechny administrátory cloudové služby                                                                                                                                                                                     | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.9.2                                         |          |          | X        | X        | X        | X        |          |
| Možnost průběžné replikace dat do prostředí on-premise, a dále možnost hromadného importu/exportu dat na paměť. médiích                                                                                                                                       | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.17, Vyhláška č. 316/2014 Sb. §26            |          | X        | X        | X        | X        | X        | X        |
| Bezpečnostní prověrky administrátorů nebo bezp. způsobilost dle §80-§87 zák. č. 412/2005 Sb.                                                                                                                                                                  | bezpečnostní opatření        | bezpečnost eGC, 412 | 412/2005 Sb. §80-§87                                    |          |          |          | X        |          |          |          |
| Auditní práva SOC 1 (SSAE16/ISAE 3402) Type II nebo ekvivalent                                                                                                                                                                                                | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.18, Vyhláška č. 316/2014 Sb. §15            |          |          | X        | X        |          |          |          |
| Auditní práva SOC 2 (AT101) Type II nebo ekvivalent                                                                                                                                                                                                           | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.18, Vyhláška č. 316/2014 Sb. §15            |          |          | 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 umožnit zákazníkovi provedení vlastních externích penetračních testů | bezpečnostní opatření        | bezpečnost eGC/ZoKB | ISO 27001 A.18, A.12; Vyhláška č. 316/2014 Sb. §15, §24 |          |          | X        | X        | X        | X        |          |
| Bezpečnostní monitoring síťového připojení služby přes CMS 2.0                                                                                                                                                                                                | bezpečnostní opatření        | bezpečnost eGC      | ISO 27017 CLD 12.4.5                                    | X        | X        | X        | X        | X        | X        |          |
| Architektura - využití kontejnerové technologie dle výsledků anal. rizik (separ. tenantů)                                                                                                                                                                     | bezpečnostní opatření        | bezpečnost eGC      | ISO 27001 A.13.1.3; ISO 27017 CLD 9.5.1                 |          |          | X        | X        | X        | X        |          |

## Bezpečnostní monitoring



## Bezpečnostní monitoring

### Výchozí pozice

- Existuje zkušenost z napojování KII/VIS MV na Dohledové centrum eGov
- Díky napojování již existující zkušený tým analytiků
- **Dohledové centrum eGOV již dnes reálně garantuje bezpečnost CMS a ITS**

### Spolupráce v rámci bezpečnosti eGC s

- Organizace využívající eGC / CMS
- Poskytovatelé služeb eGC (zejména SeGC)
- s Bezp. dohledy organizací z důvodu identifikace a řešení problémů a koordinace
- s Výjimkami mimo eGC (využívající CMS)
- s NCKB
- s uživatelem služeb – avíza, doporučení, ...

### Vize rozvoje služeb pro eGOV/eGC

- Možnost bezpečnostního dohledu na úrovni OS, DB a aplikační vrstvě i v Cloudu
- Možnost monitoringu přístupu na internet pro End Pointy – kategorizační proxy, reputační analýza objektů v internetu
- Monitoring vybraných End Pointů pomocí EDR (End Point Detection & Response)
- Možnost napojení lokálního SIEM na Bezp. dohledy
- Detailní práce s informacemi o datových tocích – detekce a analýza anomálií
- Povýšení ochrany pro volumetrické útoky
- Forenzní analýza
- Incident Response Team

### Výhody tohoto řešení

- CMS je nejen komunikační rozhraní, ale díky Bezpečnostním dohledům i „bezpečná hradba“ proti útokům zvenčí
- **Pro Dohledové centrum eGOV neznamena revoluční změnu, ale rozšíření služeb**
- Centrální místo pro pracovní koordinaci při řešení bezpečnostních problémů eGC (kompetenčně není konkurence NCKB)

## Priority a rozhraní týmu Bezpečnost v projektu eGC

- 1. Dopracovat metodiku zařazování ISVS do úrovní dopadů
    - Včetně pilotních testů hodnocení (MPO, SZR, MěÚ Kladno, MZe)
  - 2. Dopracovat výběr bezpečnostních opatření
    - Ověřování souladu primárně cestou průmyslových standardů a auditů
  - 3. Pravidla pro bezpečnostní monitoring na připojení k CMS 2.0
    - Centrální dohled v synergii s dohledem OVM a soukromého sektoru
- 
- Rozhraní na tým Provoz/Obsah:
    - Úroveň bezpečnosti jako atribut služby v rámci Katalogu služeb eGC
    - Požadavky na SLA a smluvní podmínky
  - Rozhraní na tým Organizace/Procesy:
    - Metodika zařazování do úrovní dopadů / úrovní bezpečnosti
    - Bezpečnost jako kvalifikační kritérium vstupu do Katalogu služeb eGC



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky



**DĚKUJI ZA POZORNOST**



# **Ekonomické aspekty cloudových služeb**

**Ekonomický tým**

**Ing. Michal Pešek, Martin Dolný, Petr Leština**

## **METODIKA TCO**

- **Přehledné vymezení (definice) všech relevantních nákladů**, které jsou uplatňovány jak při pořízení tak při provozu ICT služeb v režimu on-premise (tzn. Pořízení veškerého HW a SW potřebného pro poskytování dané ICT služby do vlastního majetku.)
- **Popis nákladových položek**, který bude plnit roli návodu a umožní OVM stanovit relevantní 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 OVM. Tyto údaje mají doporučující charakter a vycházejí z příkladů dobré praxe, zkušeností některých OVM 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, která bude **podkladem pro výběrové řízení** a následné soutěžení ICT služby.

## PRINCIPY METODIKY

- Forma metodiky je založená na přehledném kalkulátoru nákladů ICT služeb, umístěných v logických nákladových skupinách. Nákladové skupiny vycházejí z metodiky procesního modelování agend (více v kapitole vstupní údaje.)
- Kalkulace TCO podle Metodiky a odůvodnění ekonomické výhodnosti té které varianty je povinným vstupem před každým plánovaným pořízením ICT služby u všech OVM.
- Metodika vychází z vybraných analyzovaných obdobných návodů na kalkulaci nákladů ICT služeb ve státní správě a navazuje hlavně na Metodiku výpočtu TCO ICT služeb veřejné správy, vypracovanou Odborem hlavního architekta Ministerstva vnitra ČR (verze 3.61 z 15. 1. 2016) – dále jen “Metodika OHA”.

## **STRUTURA NÁKLADŮ**

### **Souhrnná položka modelu TCO - nákladová kategorie**

**A. Předběžné analýzy, tvorba zadání, výběr řešení a dodavatele – náklady nákupního procesu**

**B. Nákup SW a HW pro projekt (ne v případě SaaS)**

**C. Analýza, vývoj, implementace a zkušební provoz**

**D. Provoz a podpora řešení HW a SW (ne v případě SaaS)**

**E. Hardware/Software údržba a průběžné úpravy (ne v případě SaaS)**

**F. Projekty postupné inovace a zlepšování (pokud se uskutečnily)**

**G. Projekty upgrade (pokud se uskutečnily)**

**H. Zvýšené náklady užívání řešení (pokud se vyskytly)**

**I. Konzervace a ukončení řešení (u posuzovaných řešení ještě nenastala)**

**X. Náklady na předplatné ICT služby, plus všechny odpovídající přímé int. náklady (pouze SaaS)**

**Z. Ostatní, k fázi životního cyklu nepřiraditelné náklady**

## KALKULACE TCO

- Pro účely kalkulace TCO je k dispozici eGC Cloud kalkulátor. Jedná se o jednotný nástroj pro kalkulace TCO, úspor a/nebo ztrát při provozu služby v modelu on-premise a cloudu. Při jeho tvorbě byly vzaty do úvahy následující předpoklady:
- Kalkulace předpokládá 5-leté období TCO
- Porovnání je mezi modelem „on-premise“ a „cloudem“. On-premise lze chápat tak, že služba je „seskládána“ z komponent pořízených nákupem a zprovozněna formou systémové integrace. Cloud poskytuje analogicky stejnou službu jako hotovou a připravenou k použití.
- Cloud služba se rozumí IaaS, PaaS nebo SaaS; dále označované jako XaaS
  - TCO kalkulátor tvoří
  - Úvodní data
  - Vstupní data on-premise
  - Vstupní data cloud
  - Výsledky porovnání

## VSTUPNÍ DATA ON-PREMISE

Základ tvoří položkové parametry, které jsou stavebními kameny IT služby. V obecné rovině reprezentují:

/1/ Hardware

/2/ Software

/3/ Datové centrum & Networking

/4/ Lidské zdroje

/5/ ITIL disciplíny (Incident, Problem, Change management)

## VSTUPNÍ DATA CLOUD

Základ tvoří poplatek za službu a doplňkové služby nezahrnuté v základní cloudové službě (tzv. Add on services):

/1/ Poplatek za cloud službu

/2/ Lokální add-on služby nezahrnuté do cloudových služeb

## VÝSLEDKY POROVNÁNÍ

Porovnání obou kalkulací v horizontu 5 let a kalkulace úspor/ztrát při provozu v cloudu.



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky



# DĚKUJEME ZA POZORNOST



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky

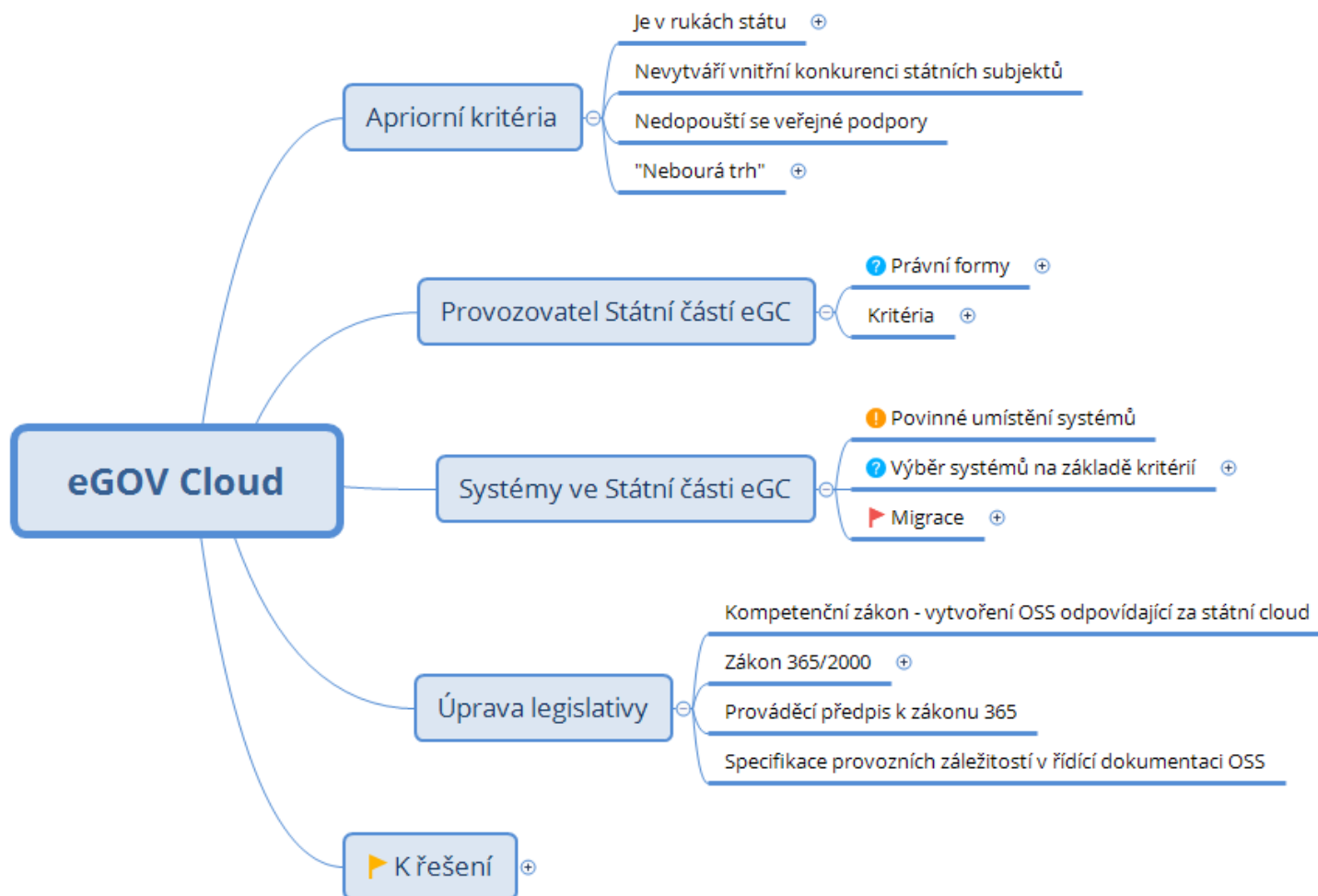


# Legislativní zakotvení eGC

Legislativní tým

**Bc. Tomáš Bezouška**

## Současný stav ... rozpracovanost



## Východiska pro budování eGC-S

**Pro úvahy o legislativním řešení byla stanovena následující východiska:**

- eGC-S je plně v rukách státu
- Vnitřní konkurence státních subjektů není žádoucí
- Nehrozí problém s veřejnou podporou
- Není poškozován komerční cloudový trh

## *Systémy a jejich zařazení do eGC-S*

### **Jaké systémy budou v eGC-S:**

- Výhradně (?) systémy provozované subjekty státní správy
- Určení systémů na základě kritérií
  - Využití výstupů PT-B
  - Provázání s kritérii dle ZKB
- Otevřená otázka: „migrovatelnost“ systémů

## *Možné právní formy správce/provozovatele eGC-S*

### **Varianty přicházející v úvahu:**

- Var 1: Státní podnik (SP)
- Var 2: Organizační složka státu (OSS)
  - Var 1a: Stávající OSS
  - Var 1b: Nová dedikovaná OSS
- Var 3: kombinace OSS / SP
  - Var 3a: OSS / SP
  - Var 3b: OSS / SP1, SP2, ...

## *Možné právní formy správce/provozovatele eGC-S*

### **Kritéria pro hodnocení a výběr varianty:**

- Možnost čerpání služeb jednotlivými OSS bez tendru
- Schopnost řídit efektivní čerpání poskytovaných služeb
- Schopnost řídit kvalitu poskytovaných služeb
- Schopnost zaměstnat (zaplatit) odborníky za tržní ceny
- Schopnost financovat investice a provoz
- Schopnost řídit nákladovou efektivitu

## *Možné právní formy správce/provozovatele eGC-S*

Rozhodnutí o volbě varianty je rozhodnutí politické, PT-LP předloží rozhodovací model vedení PS a předpokládá eskalaci na úroveň MV ČR, resp. Vlády ČR

## Úprava legislativy v souvislosti s eGC-S

### **Pro eGC-S předpokládáme následující legislativní změny:**

- Kompetenční zákon
  - Vytvoření OSS odpovídající za eGC-S
  - Současně plní roli ŘOeGC pro komerční cloud
- Zákon 365/2000 Sb.
  - Nová sekce Sdílené služby
  - Definice sdílených služeb (cloudu)
  - Vytvoření OSS, vymezení vztahu OSS-SP
- Prováděcí předpis k zákonu 365/2000 Sb.
- Specifikace provozních záležitostí v řídicí dokumentaci OSS



*... děkuji za pozornost a čas,  
přeji hezký den*

**Tomáš Bezouška**

Úřad vlády České republiky, Sekce pro podporu Rady pro vědu, výzkum a inovace

[tomas.bezouska@vlada.cz](mailto:tomas.bezouska@vlada.cz)

GSM: +420 724 838 866



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky



# Pravidla a procedury eGC

Výstup týmu Organizace a procesy

**prof. Ing. Jiří Voříšek**

## Pravidla eGC

eGovernment Cloud (eGC) se skládá ze dvou částí – státního cloudu a komerčního cloudu. Státní cloud je tvořen ICT službami ověřených datových center státu, jejichž majetek je pod kontrolou státu a pracovníci jsou zaměstnanci státu.

Komerční cloud je tvořen ICT službami ověřených datových center komerčních subjektů a jejich ověřenými službami.

Ověřování (certifikaci) datových center a služeb eGC provádí ŘOeGC.

Ve státním cloudu budou provozovány ty ICT služby, jejichž provozování privátními subjekty není z důvodů bezpečnosti možné (tzv. ICT služby kritického bezpečnostního charakteru). Všechny ostatní služby budou poskytovány komerčním cloudem.

Provozovatelé státní části eGC si nebudou konkurovat mezi sebou, ani s poskytovateli komerční části eGC. 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.

Provozovatelé komerční části eGC si budou mezi sebou konkurovat, tzn., že ŘOeGC bude při řízení komerčního cloudu postupovat tak, aby každý typ sdílené ICT služby byl nabízen více provozovateli (tj. aby se využívaly decentralizované sdílené systémy). Cílem je vyhnout se „vendor lock-in“ a zajistit konkurenční tržní prostředí.

## Pravidla eGC

eGovernment Cloud (eGC) se skládá ze dvou částí – státního cloudu a komerčního cloudu.

Státní cloud je tvořen ICT službami ověřených datových center státu, jejichž majetek je pod kontrolou státu a pracovníci jsou zaměstnanci státu.

Komerční cloud je tvořen ICT službami ověřených datových center komerčních subjektů a jejich ověřenými službami.

Ověřování (certifikaci) datových center a služeb eGC provádí ŘOeGC.

Ve státním cloudu budou provozovány ty ICT služby, jejichž provozování privátními subjekty není z důvodů bezpečnosti možné (tzv. ICT služby kritického bezpečnostního charakteru).

Všechny ostatní služby budou poskytovány komerčním cloudem.

Provozovatelé státní části eGC si nebudou konkurovat mezi sebou, ani s poskytovateli komerční části eGC. 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.

Provozovatelé komerční části eGC si budou mezi sebou konkurovat, tzn., že ŘOeGC bude při řízení komerčního cloudu postupovat tak, aby každý typ sdílené ICT služby byl nabízen více provozovateli (tj. aby se využívaly decentralizované sdílené systémy). Cílem je vyhnout se „vendor lock-in“ a zajistit konkurenční tržní prostředí.

## Pravidla eGC

Státní část eGC poskytuje služby, které nejde poskytovat v komerční části eGC, proto jeho zákazníci (OVM) objednávají jeho služby bez potřeby veřejné zakázky.

Na nákup služeb komerční části eGC jsou aplikovány pravidla ZVZ (Dynamický nákupní systém – DNS).

ICT služby eGC jsou nabízeny jednotlivým OVM přes portál eGC.

ICT služby jsou dodávány a garantovány poskytovatelem zákazníkovi (OVM) na základě SLA (smlouva na dodávku ICT služeb, Service Level Agreement)

Za porušení SLA je poskytovatel sankcionován.

SLA mezi zákazníkem a poskytovatelem komerčního cloudu bude vždy na dobu určitou (maximální doba smlouvy bude stanovena v daném Soutěžním rámci) s jasnou možností ukončení služby a s možným přechodem k jinému poskytovateli služby (vč. povinné součinnosti původního poskytovatele při ukončení a migraci dat). Cílem omezené doby platnosti smlouvy je využít postupně klesajících cen ICT služeb na ICT trhu a vyhnout se „vendor lock-in“.

Za spotřebovávané služby zákazníci platí.

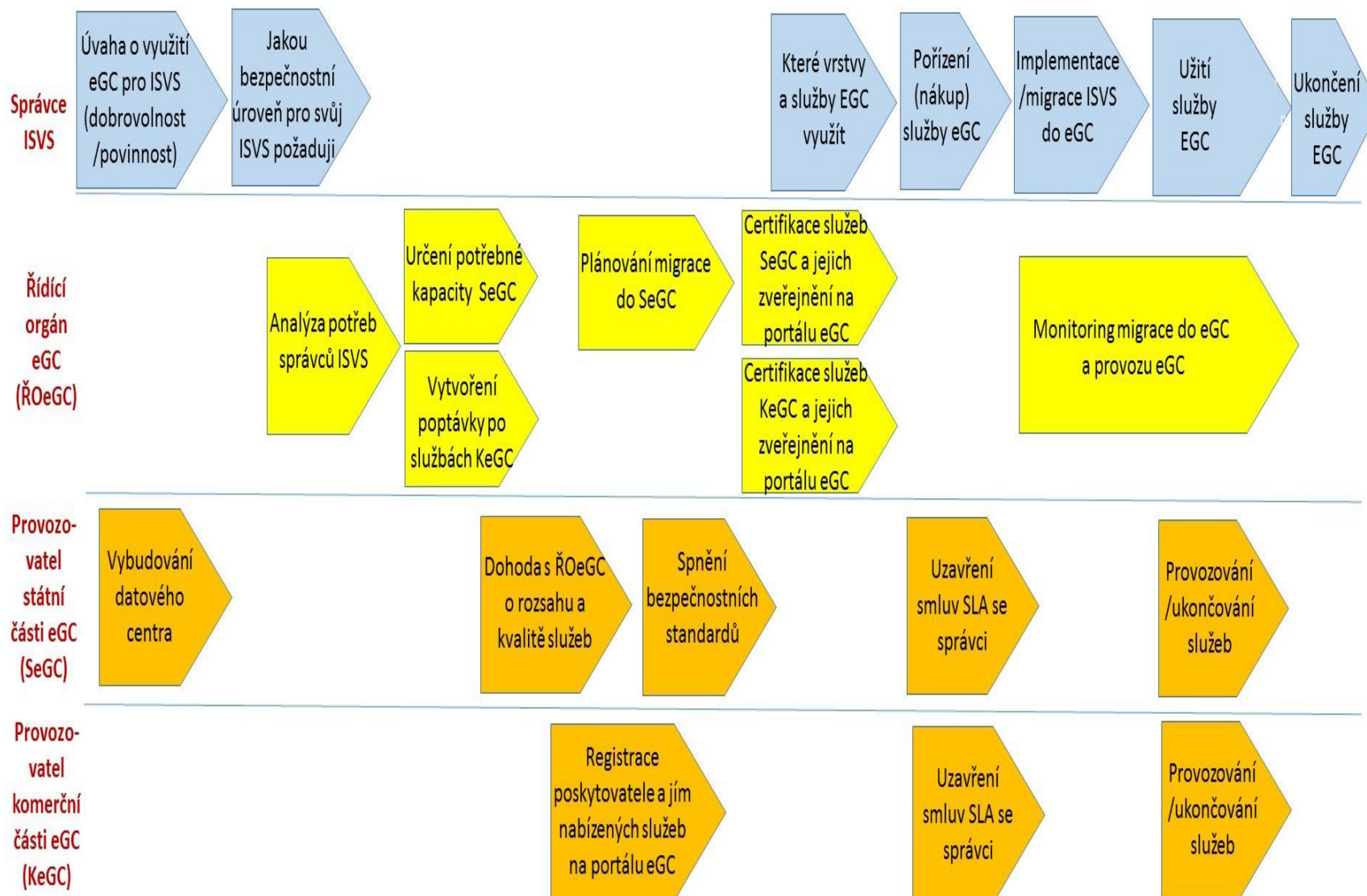
**Migrace informačních systémů do eGC bude pro kraje, města, obce a dále pro ČNB, zpravodajské služby a bezpečnostní sbory státu dobrovolná. Pro ostatní státní instituce platí tato pravidla:**

| 1. etapa do r. 20xx (např. do r. 2020)                     | 1. etapa po r. 20xx                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Migrace do eGC je pro všechny státní instituce dobrovolná. | <p>Migrace do eGC bude pro státní instituce probíhat na základě principu cloud first, tj. jestliže dožije technologická infrastruktura stávajícího informačního systému nebo se staví nový informační systém, pak:</p> <ol style="list-style-type: none"><li>(1) Jestliže bude v nabídce eGC existovat požadovaná služba typu SaaS, nesmí instituce pořídit danou službu mimo eGC, ledaže by na základě analýzy TCO prokázala, že jí navrhované řešení je ekonomicky výhodnější.</li><li>(2) Jestliže nebude v nabídce eGC existovat požadovaná služba typu SaaS, musí instituce využít pro provoz aplikace službu IaaS, resp. PaaS, resp. službu systémové integrace, ledaže by na základě analýzy TCO prokázala, že jí navrhované řešení je ekonomicky výhodnější.</li></ol> |

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

V komerční části eGC budou již od počátku využívány všechny typy ICT služeb, tj. včetně SaaS a systémové integrace.

## Procedury eGC – hrubý pohled dle aktérů



## **Procedury eGC – společné pro státní i komerční část**

### ***Naplnění katalogu DC VS***

Provozovatelé datových center VS, které v současné době využívají státní instituce a kraje, uloží informace o svém datovém centru do katalogu DC VS (tj. včetně informací o své kapacitě a o úrovni bezpečnosti a dostupnosti, kterou jsou schopni garantovat)

**T:dd/mm/rr.**

Svoje údaje v katalogu musejí provozovatelé DC minimálně jedenkrát ročně aktualizovat.

### ***Aktualizace katalogu aktuálně provozovaných ISVS (tj. IS o ISVS)***

Věcní správci informačních systémů VS, které jsou vymezeny zákonem 365 (agendové IS, spisová služba, ERP, HR a e-mail), uloží do IS o ISVS (tj. do katalogu aktuálně provozovaných ISVS) informace o svém IS v požadované struktuře, tj. včetně zařazení IS do jedné ze čtyř kategorií bezpečnosti a spolehlivosti (nízká, střední, vysoká, kritická), datovém centru, ve kterém je IS provozován, a včetně případného **požadavku na přesun IS do eGC** (viz první dva podprocesy u Správce ISVS na obrázku)

**T:dd/mm/rr**



MINISTERSTVO VNITRA  
ČESKÉ REPUBLIKY



Ministerstvo financí  
České republiky



# DĚKUJI ZA POZORNOST