eGOVERNMENT CLOUD_

ZÁPISEM DO KATALOGU TO NEKONČÍ_

HELENA ULRYCHOVÁ_

VEDOUCÍ ODDĚLENÍ eGOVERNMENT CLOUDU_

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

PETR KOPŘIVA

VEDOUCÍ ODDĚLENÍ REGULACE DODAVATELŮ INFORMAČNÍCH TECHNOLOGIÍ

NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

NÚKIB

ISSS 2025_
12. 5. 2025_

eGOVERNMENT CLOUD_

- Definice a regulace
- Povinnosti pro orgány veřejné správy
- Povinnosti pro poskytovatele
- Katalog cloud computingu
- Státní poskytovatel cloud computingu
- Zápisem to nekončí …

CLOUD COMPUTING_

- **zákon č. 365/2000 Sb., o informačních systémech veřejné správy**
  - informační systémy veřejné správy
  - orgány veřejné správy

- **zajištění provozu** informačního systému veřejné správy nebo jeho části prostřednictvím **dálkového přístupu** k **sdílenému** technickému nebo programovému prostředku, který je **zpřístupněný poskytovatelem** cloud computingu a **nastavitelný** správcem informačního systému veřejné správy

VÝJIMKY

DŮVODY REGULACE_

- využití cloudových služeb jak v soukromém, tak ve veřejném sektoru rychle roste

- **nová rizika:** 
  - místo zpracování dat
  - přístup cizozemských orgánů k datům
  - velká závislost na poskytovateli a omezené možnosti prověření poskytovatele

POVINNOSTI PRO OVS ZE ZoISVS_

- Orgán veřejné správy může využívat **pouze** cloud computing, který je poskytovaný:
  - poskytovatelem státního cloud computingu nebo poskytovatelem cloud computingu **zapsaným v katalogu cloud computingu,**
  - v rámci vertikální nebo horizontální spolupráce nebo obecné výjimky z povinnosti zadat veřejnou zakázku
  - **VÝJIMKY**

Pokud využívaný CC **nesplňuje podmínky ZoISVS**, musí OVS **do 12 měsíců** ukončit jeho využívání

BEZPEČNOSTNÍ ÚROVNĚ

Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

- Stanoví bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci
- 4 bezpečnostní úrovně:

NÍZKÁ
STŘEDNÍ
VYSOKÁ
KRITICKÁ

- Stanovení bezpečnostní úrovně dle úrovně dopadu kybernetického bezpečnostního incidentu

Úroveň dopadu	Oblast dopadu								
	A. Bezpečnost a zdraví lidí	B. Ochrana osobních údajů	C. Trestněprávní řízení	D. Veřejný pořádek	E. Mezinárodní vztahy	F. Řízení a provoz	G. Důvěryhodnost	H. Finanční model	I. Zajišťování služeb

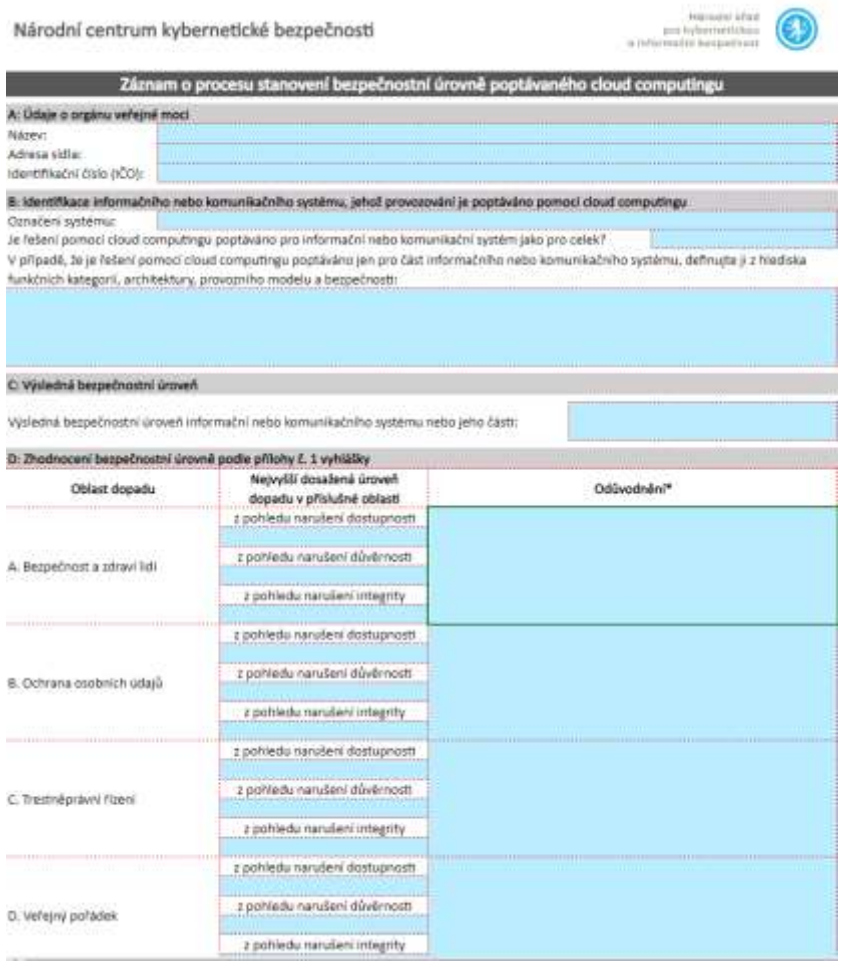
DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

BEZPEČNOSTNÍ ÚROVNĚ

Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

Základní principy hodnocení dopadů:

- Nezkoumat příčiny narušení bezpečnosti
- Identifikovat opravdu nejhorší možné scénáře
- Neřešit pravděpodobnost výskytu těchto scénářů
- Neuvažovat jakákoliv bezpečnostní opatření



Národní centrum kybernetické bezpečnosti

Záznam o procesu stanovení bezpečnostní úrovně poptávaného cloud computingu

A: Údaje o orgánu veřejné moci

Název:
Adresa sídla:
Identifikační číslo (IČO):

B: Identifikace informačního nebo komunikačního systému, jehož provozování je poptáváno pomocí cloud computingu

Označení systému:
Je řešení pomocí cloud computingu poptáváno pro informační nebo komunikační systém jako pro celek?
V případě, že je řešení pomocí cloud computingu poptáváno jen pro část informačního nebo komunikačního systému, definujte ji z hlediska funkčních kategorií, architektury, provozního modelu a bezpečnosti:

C: Výsledná bezpečnostní úroveň

Výsledná bezpečnostní úroveň informační nebo komunikačního systému nebo jeho části:

D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky

Oblast dopadu	Nejvyšší dosažená úroveň dopadu v příslušné oblasti	Odůvodnění*
A. Bezpečnost a zdraví lidí	z pohledu narušení dostupnosti	
	z pohledu narušení důvěrnosti	
	z pohledu narušení integrity	
B. Ochrana osobních údajů	z pohledu narušení dostupnosti	
	z pohledu narušení důvěrnosti	
	z pohledu narušení integrity	
C. Trestněprávní řízení	z pohledu narušení dostupnosti	
	z pohledu narušení důvěrnosti	
	z pohledu narušení integrity	
D. Veřejný pořádek	z pohledu narušení dostupnosti	
	z pohledu narušení důvěrnosti	
	z pohledu narušení integrity	

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

BEZPEČNOSTNÍ ÚROVNĚ

Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci

- Výsledná bezpečnostní úroveň

  = **nejvyšší úroveň dopadu**

- Nejvyšší stanovená bezpečnostní úroveň informačního nebo komunikačního systému jako celku musí být stanovena alespoň pro jednu část informačního nebo komunikačního systému

D: Zhodnocení bezpečnostní úrovně podle přílohy č. 1 vyhlášky		
Oblast dopadu	**Nejvyšší dosažená úroveň dopadu v příslušné oblasti**	**Odůvodnění**
A. Bezpečnost a zdraví lidí	z pohledu narušení dostupnosti	*Narušení dostupnosti, důvěrnosti či integrity Evidence žadatelů a uživatelů sociálních služeb (dále jen "Evidence") nemůže přímo jakkoli způsobit zranění jednotlivce ani skupiny lidí.* *Evidence slouží pouze jako jmenný seznam osob, není zde tedy jakákoli možnost ohrožení jejich zdraví či bezpečnosti.*
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	NÍZKÁ	
	z pohledu narušení integrity	
	NÍZKÁ	
B. Ochrana osobních údajů	z pohledu narušení dostupnosti	*Narušení bezpečnosti informací v rámci Evidence může negativně ovlivnit poptávaný cloud computing, který naplňuje dvě a více kritérií z druhé skupiny kritérií pro oblast dopadu B. Ochrana osobních údajů. Konkrétně je naplněno kritérium a) a b) z druhé skupiny kritérií, jelikož jsou zpracovávány zvláštní kategorie osobních údajů uživatelů systému a tímto zpracováním bude určitě dotčeno více než 10000 subjektů údajů.*
	NÍZKÁ	
	z pohledu narušení důvěrnosti	
	VYSOKÁ	
	z pohledu narušení integrity	
	VYSOKÁ	

POVINNOSTI PRO OVS_ PŘED VYUŽÍVÁNÍM CLOUD COMPUTINGU 2_

Stanovení bezpečnostní úrovně

- **vyhláška č. 315/2021 Sb.,** o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci
  - **podmínka do veřejné zakázky**

Dekompozice ISVS

- dobrovolné
- cílem je zařadit každou komponentu do nejvhodnější bezpečnostní úrovně a využít tak **optimální technologie** (a optimální finanční náklady)

Předběžné posouzení plánovaných nákladů výhodnosti zvoleného řešení

- **vyhláška č. 360/2023 Sb.,** o dlouhodobém řízení informačních systémů veřejné správy

Smluvní zajištění některých bezpečnostních pravidel

- **vyhláška č. 190/2023 Sb.**, o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
  - **dostupnost služeb; nakládání s daty; právo odstoupit od smlouvy; exit plán**

BEZPEČNOSTNÍ PRAVIDLA

Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

- Stanovuje obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
- Každá z bezpečnostních úrovní dle vyhlášky o bezpečnostních úrovních má příslušná bezpečnostní pravidla
- Jejich účelem je zajištění bezpečnosti informací při využívání služeb cloud computingu OVM

- Výkladové zúžení NÚKIB – stejná množina povinných osob jako v případě ZoISVS

BEZPEČNOSTNÍ PRAVIDLA

Vyhláška č. 190/2023 Sb., o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu

1. Obecné podmínky pro službu cloud computingu
2. Organizace bezpečnosti informací
3. Politiky
4. Fyzická bezpečnost
5. Zajištění provozu služby cloud computingu
6. Správa identit a řízení přístupu
7. Správa klíčů a šifrování
8. Zabezpečení komunikace
9. Přenositelnost, propojení a exit strategie
10. Nákup vývoj a úprava informačních systémů
11. Řízení dodavatelů
12. Správa kybernetických bezpečnostních událostí a incidentů
13. Řízení kontinuity činností
14. Soulad s předpisy a audit
15. Žádosti cizozemských orgánů o zpřístupnění nebo předání dat

POVINNOSTI PRO OVS_ PŘI VYUŽÍVÁNÍ CLOUD COMPUTINGU_

Zajištění bezpečnostních pravidel

- **vyhláška č. 190/2023 Sb.**, o bezpečnostních pravidlech pro orgány veřejné moci využívající služby poskytovatelů cloud computingu
- podle dané bezpečnostní úrovně

Zápis využívaného cloud computingu do katalogu CC a poskytování informací o finančním objemu vynaloženém na CC

- § 6x a § 6y **ZoISVS**

POVINNOSTI PRO POSKYTOVATELE_

- Zápis **poskytovatele** cloud computingu do katalogu cloud computingu – § 6q a § 6r **ZoISVS**
- Zápis **nabídky** cloud computingu do katalogu cloud computingu – § 6t a § 6u **ZoISVS**

- **Vyhláška č. 316/2021 Sb.**, o některých požadavcích pro zápis do katalogu cloud computingu

ZAHÁJIT PROCES ZÁPISU VČAS

DIGITÁLNÍ A INFORMAČNÍ AGENTURA_

POŽADAVKY NA POSKYTOVATELE

- § 6m ZoISVS – Požadavky na poskytovatele
  - *a) způsobilé zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy,*
  - *b) bezúhonné v rozsahu bezúhonnosti požadované po kvalifikovaném správci kvalifikovaného systému elektronické identifikace,*
  - *c) způsobilé pro poskytnutí cloud computingu orgánu veřejné správy z hlediska **veřejného pořádku, bezpečnosti a dodržování práv třetích osob**.*

- § 6n ZoISVS – Požadavky na služby
  - *b) který **umožňuje dosažení** alespoň **základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací** orgánu veřejné správy,*
  - *c) který umožňuje orgánu veřejné správy postupovat podle **bezpečnostních pravidel** pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost,*
  - *d) jehož **bezpečnostní úroveň je stejná nebo vyšší** než bezpečnostní úroveň informačního systému veřejné správy nebo jeho části, k zajištění jehož provozu je využíván,*

POŽADAVKY PRO ZÁPIS DO KATALOGU CC

Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu

- Sada bezpečnostních požadavků a podmínek, které musí poskytovatel CC služeb splnit, aby mohl dodávat orgánům veřejné správy
- Cloudové služby rozděleny do 4 úrovní podle požadavku na bezpečnost

Strana 3770 Sbírka zákonů č. **316** / 2021 Částka 140

316

VYHLÁŠKA

ze dne 24. srpna 2021

o některých požadavcích pro zápis do katalogu cloud computingu

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle § 12 odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 261/2021 Sb., (dále jen „zákon"):

§ 1

Předmět úpravy

Tato vyhláška stanoví

a) požadavky na způsobilost poskytovatele cloud computingu (dále jen „poskytovatel") zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy podle § 6m odst. 1 písm. a) zákona,

b) požadavky na dosažení základní úrovně ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy nakládaným cloud computingem podle § 6n písm. b) zákona,

c) seznam certifikací a auditů pro oblast ochrany důvěrnosti, integrity a dostupnosti informací podle § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a § 6t odst. 7 písm. c) zákona, doklady o jejich splnění a intervaly pro předkládání těchto do-

§ 6t odst. 6 písm. g) a § 6t odst. 7 písm. h) zákona.

§ 2

Základní pojmy

Pro účely této vyhlášky se rozumí

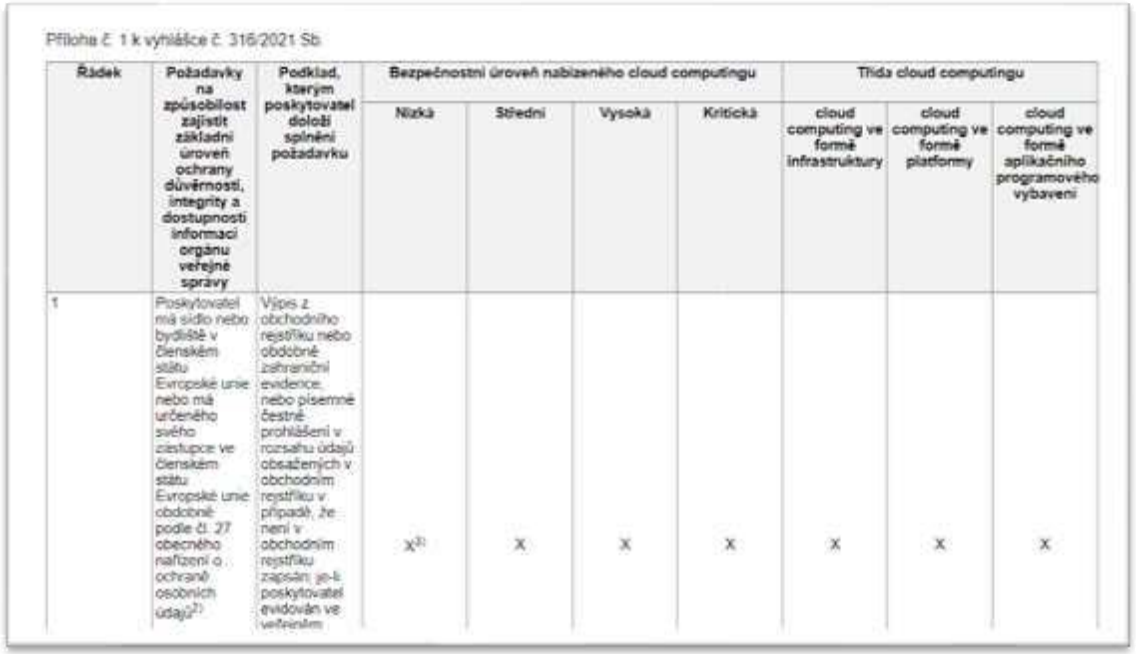
a) zákazníkem orgán veřejné správy využívající službu cloud computingu,

b) uživatelem ten, kdo službu cloud computingu prostřednictvím systému orgánu veřejné správy využívá nebo ji nastavuje,

c) zákaznickými daty všechna data, která jsou uživatelem poskytnuta poskytovateli v průběhu užívání služby cloud computingu,

d) zákaznickým obsahem textová, zvuková, audiovizuální, obrazová nebo jiná data, která byla uživatelem do služby cloud computingu vložena, a to bez jejich metadat, a indexy k těmto datům,

e) provozními údaji data vygenerovaná nebo odvozená poskytovatelem v souvislosti s poskyto-



Příloha č. 1 k vyhlášce č. 316/2021 Sb.

Řádek	Požadavky na způsobilost zajistit základní úroveň ochrany důvěrnosti, integrity a dostupnosti informací orgánu veřejné správy	Podklad, kterým poskytovatel doloží splnění požadavku	Bezpečnostní úroveň nabízeného cloud computingu				Třída cloud computingu		
			Nízká	Střední	Vysoká	Kritická	cloud computing ve formě infrastruktury	cloud computing ve formě platformy	cloud computing ve formě aplikačního programového vybavení
1	Poskytovatel má sídlo nebo bydliště v členském státu Evropské unie nebo má určeného svého zástupce ve členském státu Evropské unie obdobně podle čl. 27 obecného nařízení o ochraně osobních údajů[2)]	Výpis z obchodního rejstříku nebo obdobné zahraniční evidence, nebo písemné čestné prohlášení v rozsahu údajů obsažených v obchodním rejstříku v případě, že není v obchodním rejstříku zapsán, je-li poskytovatel evidován ve veřejném	x[3)]	x	x	x	x	x	x

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

KATALOG CLOUD COMPUTINGU_

1. Poptávky OVS

- Společná
- Individuální

2. Poskytovatelé CC

- „Komerční“ – 1. - 3. bezpečnostní úroveň
- Státní – 4. bezpečnostní úroveň, všechny kritické IS, část významných IS

3. Nabídky CC

- Konkrétní služby CC

4. Využívaný CC

- Smlouva s poskytovatelem CC
- Finanční objem vynaložený na CC

NÁSTROJ PRO VYHLEDÁVÁNÍ V KATALOGU CC_

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

KATALOG CLOUD COMPUTINGU_

Jedná se o vyhledávací nástroj nad katalogem cloud computingu, který je dostupný na webu Digitální a informační agentury.

Aktualizováno:
4. května 2025

Bezpečnostní úroveň zapsaných služeb:

- "1" - Nízká
- "2" - Střední
- "3" - Vysoká
- "4" - Kritická

Počet zapsaných poskytovatelů v katalogu:

147

Počet poskytovatelů se zapsanou nabídkou:

52

Z toho:

13

materiální poskytovatelé

Počet typů poptávaných služeb:

67

IaaS a PaaS

112

SaaS a smíšené modely

Počet zapsaných služeb v katalogu

5 420

přímý prodej služeb od přeprodejců

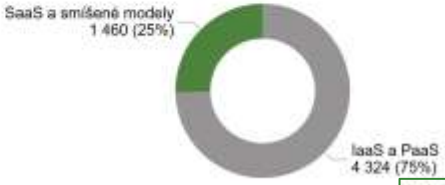
169

přímý prodej služeb od materiálních poskytovatelů

195

nepřímý prodej služeb od materiálních poskytovatelů

Počet zapsaných služeb podle unikátního ID:



Katalog služeb CC_

ID služby	Materiální poskytovatel (IČO)	Koncový prodejce (IČO)	Bezpečnostní úroveň:	Nabízeno přímo OVS?	Třída služeb	Oblast služeb	Typ služby	Základní parametry typu služby - určující
						centrálním systémem		
012-012-0010	A L I S spol. s r.o. (00672416)	A L I S spol. s r.o. (00672416)	"2" - Střední	ANO	SaaS a smíšené modely	Agendové systémy nezajišťované jednotným centrálním systémem	Portál občana - redakční systém	Nepřetržité zpřístupnění vybraných elektronických služeb občanům
012-012-0010	A L I S spol. s r.o. (00672416)	A L I S spol. s r.o. (00672416)	"2" - Střední	ANO	SaaS a smíšené modely	Agendové systémy nezajišťované jednotným centrálním systémem	Portál občana - transakční část	Formulářový systém; vazba na NIA; elektronické podání
023-023-0001	ALVAO s.r.o. (25561561)	ALVAO s.r.o. (25561561)	"3" - Vysoká	ANO	SaaS a smíšené modely	Ostatní provozní služby	Datová analytika	Analýza dat a reporting; vizualizace výsledků; práce se strukturovanými a příp. i nestrukturovanými daty

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

POSKYTOVATEL STÁTNÍHO CLOUD COMPUTINGU_

- **Státní pokladna Centrum sdílených služeb, s. p.**
  - pověřen vládou 20. 12. 2023
  - jediný může poskytovat služby kritické (4.) bezpečnostní úrovně
    - mandatorně všechny určené informační nebo komunikační systémy kritické informační infrastruktury a část významných informačních systémů podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti
  - kapacitní plán
    - do konce roku 2028 plánuje 11 OVS využít služeb SeGC pro 23 ISVS
  - služby státního cloud computingu nejsou poskytovány zdarma ☺

PROČ VYUŽÍVAT CC Z KATALOGU_

- zvýšení **bezpečnosti** ISVS – **prověřené** služby od prověřených poskytovatelů
- možnost **dekompozice** ISVS – optimální řešení
- **škálovatelnost** rozsahu odebíraných služeb – platím jen za to, co využiji
- finanční **úspora** – investiční vs provozní náklady
- **rychlost** zavádění – nabízené služby jsou již v provozu

DYNAMICKÝ NÁKUPNÍ SYSTÉM_

- **DNS na zajištění služeb cloud computingu**
  - služby třídy SaaS
  - zavedeno 18. 12. 2024
  - poskytovatel i nabídka musí být zapsáni v katalogu CC
- **Příprava vzorové smlouvy**
  - předběžné tržní konzultace
- **Příprava metodických pokynů pro zadavatele**
  - konzultace s orgány veřejné správy

ZÁPISEM DO KATALOGU TO NEKONČÍ

- **Kontroly ze strany DIA**
  - poskytovatelé
  - nabídky
    - dle přílohy č. 3 a č. 4 vyhlášky č. 316/2021 Sb.
- **Výmaz**
  - na žádost (služba, nabídka)
  - z moci úřední
- **Informační povinnost poskytovatele**
  - změna údajů vedených v katalogu
  - změna doložených podkladů
- **Aktualizace** – název, cena …
  - jinak nová žádost

CO CHYSTÁME_

- **Metodiky, návody, formuláře**
  - orgány veřejné správy
  - poskytovatelé

- **Informační systém Cloud computingu**

- **Legislativa**
  - zákon č. 365/2020 Sb.
  - vyhláška č 316/2021 Sb.

NOVELIZACE 2025

- Přesun ze ZKB do ZoISVS
  - Povinnosti zařadit do BÚ a dodržovat BP
  - Zmocnění k vyhláškám o BÚ a BP
  - Sjednocení adresátů
  - Zavedení přestupků
- Znovuvydání všech cloudových vyhlášek
  - Vlastní legislativní proces
  - U vyhlášky o požadavcích pro zápis do katalogu cloud computingu **30 dní**

PŘEHLED HLAVNÍCH NOVELIZAČNÍCH BODŮ

- Nová koncepce bezúhonnosti za přestupky
- Zpřehlednění a zlepšení UX
- Rozšíření množiny akceptovatelných auditních zpráv
- Odstranění požadavku na dostupnost zapisované služby
- Úprava požadavků na penetrační testování a skeny zranitelnosti
- Úprava požadavků na šifrování
- Explicitně uvedená povinnost dokládat čestné prohlášení, pokud není zapisovaná služba jmenovitě uvedená v daném dokumentu

KDE NAJÍT INFORMACE? DIA_

- Metodiky, návody, formuláře:
  - Metodiky, návody, formuláře - Digitální a informační agentura (gov.cz)
- Kalkulátor TCO:
  - Metodika TCO (Metodika pro výpočet celkových nákladů vlastnictví ISVS) - Digitální a informační agentura (gov.ckatz)
- Katalog CC:
  - Katalog cloud computingu - Digitální a informační agentura (gov.cz)
  - Nástroj pro vyhledávání v katalogu cloud computingu - Digitální a informační agentura (gov.cz)

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

KDE NAJÍT INFORMACE? NÚKIB

- Podpůrné materiály:

  Obecně:

  - Národní úřad pro kybernetickou a informační bezpečnost - Podpůrné materiály (gov.cz)

  Ke cloud computingu:

  - Národní úřad pro kybernetickou a informační bezpečnost - Materiály k regulaci cloud computingu (gov.cz)

- Nejčastější dotazy:
  - Národní úřad pro kybernetickou a informační bezpečnost - FAQ (gov.cz)
- Služby, které trvale ukládají data mimo EU – Úřední deska NÚKIB
  - Národní úřad pro kybernetickou a informační bezpečnost - Cloud computing - výjimky z uložení dat (gov.cz)

DĚKUJEME ZA POZORNOST

PROSTOR PRO VAŠE DOTAZY

Helena Ulrychová
helena.ulrychova@dia.gov.cz

Petr Kopřiva
petr.kopriva@nukib.gov.cz

CLOUD HOTLINE

egc@dia.gov.cz

regulace@nukib.gov.cz

DIGITÁLNÍ
A INFORMAČNÍ
AGENTURA_

NÚKIB