

Metodické usmernenie z 11.04.2025  
č. 020775/2025/oSBATA pre proces  
zaradenia cloudovej služby do katalógu  
vládných cloudových služieb(MIRRI)

|                  |                                                                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Určené pre:      | Sekcia informačných technológií verejnej správy, orgány riadenia podľa § 5 ods. 2 zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov |
| Vydáva:          | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky<br>Sekcia informačných technológií verejnej správy                                                                                         |
| Záväznosť:       | Tento dokument má záväzný charakter                                                                                                                                                                                            |
| Počet príloh:    | 12                                                                                                                                                                                                                             |
| Dátum vydania:   | 11.4.2025                                                                                                                                                                                                                      |
| Dátum účinnosti: | 15.4.2025                                                                                                                                                                                                                      |
| Schválil:        | Ing. et Ing. Martin Déneši PhD., MSc.<br>Poverený riadením sekcie informačných technológií verejnej správy<br>Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky                              |

## Obsah

|                                                                                    |    |
|------------------------------------------------------------------------------------|----|
| Obsah .....                                                                        | 1  |
| 1 Úvod .....                                                                       | 3  |
| 1.1 Dôležité skratky, výrazy a vysvetlenia .....                                   | 3  |
| 1.2 Účel dokumentu .....                                                           | 4  |
| 2 Východiská, terminológia .....                                                   | 4  |
| 2.1 Základné charakteristiky a predpoklady pre využívanie cloudových služieb ..... | 5  |
| 2.2 Modely cloudových služieb .....                                                | 6  |
| 2.3 Vzťahy a závislosti medzi jednotlivými modelmi cloudových služieb .....        | 6  |
| 2.4 Modely nasadenia cloudových služieb: .....                                     | 7  |
| 2.5 Kategórie cloudových služieb pre OVM .....                                     | 8  |
| 2.6 Doba platnosti hodnotenia poskytovanej cloudovej služby .....                  | 10 |
| 2.7 Úloha a postavenie MIRRI .....                                                 | 10 |
| 2.8 Používateľ ponúkanej cloudovej služby .....                                    | 10 |
| 2.9 Poskytovateľ ponúkanej cloudovej služby .....                                  | 10 |
| 2.10 Prevádzkovateľ ponúkanej cloudovej služby .....                               | 11 |
| 2.11 Sprostredkovateľ cloudovej služby .....                                       | 11 |
| 2.12 Poskytovateľ podpory ako služby .....                                         | 11 |
| 3 Životný cyklus cloudovej služby .....                                            | 12 |
| 3.1 Žiadosť o zápis ponúkanej cloudovej služby do KsVC .....                       | 12 |
| 3.1.1 Rozdelenie ponúkaných cloudových služieb do jednotlivých kategórií .....     | 13 |
| 3.1.1.1 Kategória U1 .....                                                         | 13 |
| 3.1.1.2 Kategória U2 .....                                                         | 13 |
| 3.1.1.3 Kategória U3 .....                                                         | 14 |
| 3.1.1.4 Kategória U4 .....                                                         | 14 |
| 3.1.2 Uznávanie certifikácií tretích strán .....                                   | 14 |
| 3.1.3 Preukázanie kvalifikácie pre poskytovanie služby .....                       | 15 |
| 3.2 Proces hodnotenia služby .....                                                 | 16 |
| 3.2.1 Hodnotiteľ .....                                                             | 16 |
| 3.2.2 Pôsobnosť hodnotiteľa pre jednotlivé kategórie ponúkanej CS .....            | 16 |

|         |                                                                         |    |
|---------|-------------------------------------------------------------------------|----|
| 3.2.3   | Formulár pre samohodnotenie pre kategóriu U1.....                       | 18 |
| 3.2.4   | Dotazníkový formulár pre hodnotenie pre kategóriu U2, U3, U4 .....      | 19 |
| 3.2.5   | Hodnotenie poskytovanej cloudovej služby .....                          | 24 |
| 3.2.5.1 | Zjednodušený spôsob hodnotenia .....                                    | 24 |
| 3.3     | Zápis hodnotenej cloudovej služby do Katalógu cloudových služieb .....  | 25 |
| 3.4     | Monitoring a kontrola kvality poskytovania CS .....                     | 26 |
| 3.4.1   | Roly a povinnosti MIRRI .....                                           | 26 |
| 3.4.2   | Proces zistenia nesúlady služby .....                                   | 27 |
| 3.5     | Ukončenie poskytovania služby .....                                     | 28 |
| 3.5.1   | Vyradenie zapísanej cloudovej služby z Katalógu cloudových služieb..... | 28 |
| 3.5.2   | Ukončenie poskytovania služby na žiadosť poskytovateľa.....             | 30 |
| 4       | Povinnosti OR pri využívaní služby zapísanej v KsVC.....                | 30 |
| 4.1     | Registrácia používania služby.....                                      | 30 |
| 5       | Prílohy.....                                                            | 30 |

# 1 Úvod

MIRRI podľa § 8 ods. 1 písm. c) zákona č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov (ďalej len „zákon“) vydáva toto metodické usmernenie na účely jednotného spôsobu výkonu riadenia v správe informačných technológií verejnej správy a centrálného riadenia informatizácie spoločnosti. Metodické usmernenie rieši procesy spojené so zápisom do evidencie vládnych cloudových služieb v zmysle zákona č. 95/2019 Z. z. §24a, odsek. 3, odsek. 4.

## 1.1 Legislatíva

- zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 69/2018 Z. z.“),
- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v znení vyhlášky Národného bezpečnostného úradu č. 264/2023 Z. z. (ďalej len „vyhláška NBÚ č. 362/2018 Z. z.“),
- zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 95/2019 Z. z.“),
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 179/2020, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy (ďalej len „vyhláška ÚPVII č. 179/2020 Z. z.“),
- vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy v znení neskorších predpisov (ďalej len „vyhláška ÚPVII č. 78/2020 Z. z.“),
- vyhláška Národného bezpečnostného úradu č. 165/2018 Z. z., ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov (ďalej len „vyhláška NBÚ č. 165/2018 Z. z.“),
- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 215/2004 Z. z.“),
- ďalšie súvisiace predpisy.

## 1.2 Dôležité skratky, výrazy a vysvetlenia

**MIRRI** – Ministerstvo investícií, regionálneho rozvoja a informatizácie SR.

**Overenie súladu služby** – overenie súladu cloudovej služby s požiadavkami zákonov, vyhlášok, nariadení a metodických usmernení vydaných v SR z pohľadu bezpečnosti cloudových služieb a služieb s nimi spojených.

**Hodnotenie/Audit cloudovej služby** – Overenie súladu služby

**KsVC** – Katalóg služieb Vládneho cloudu

**CS** – Cloudová služba

**OR** – Orgán riadenia

**C, I, A** – Confidentiality, Integrity, Availability / Dôvernosť, Integrita, Dostupnosť  
– klasifikačné atribúty informačných aktív

**U** – Bezpečnostná úroveň cloudovej služby

**OR** – Orgán riadenia

**OV** – Orgán vedenia

### 1.3 Účel dokumentu

Cieľom tohto Metodického usmernenia pre proces zaradenia cloudovej služby do katalógu je ustanovenie procesu kvalifikácie cloudovej služby (ďalej len “usmernenie”).

Metodické usmernenie popisuje procesy kvalifikácie ponúkanej cloudovej služby pre Orgány riadenia (ďalej len OR), jej registrácie, hodnotenia, zaradenia do katalógu ponúkaných cloudových služieb a celý životný cyklus ponúkanej cloudovej služby.

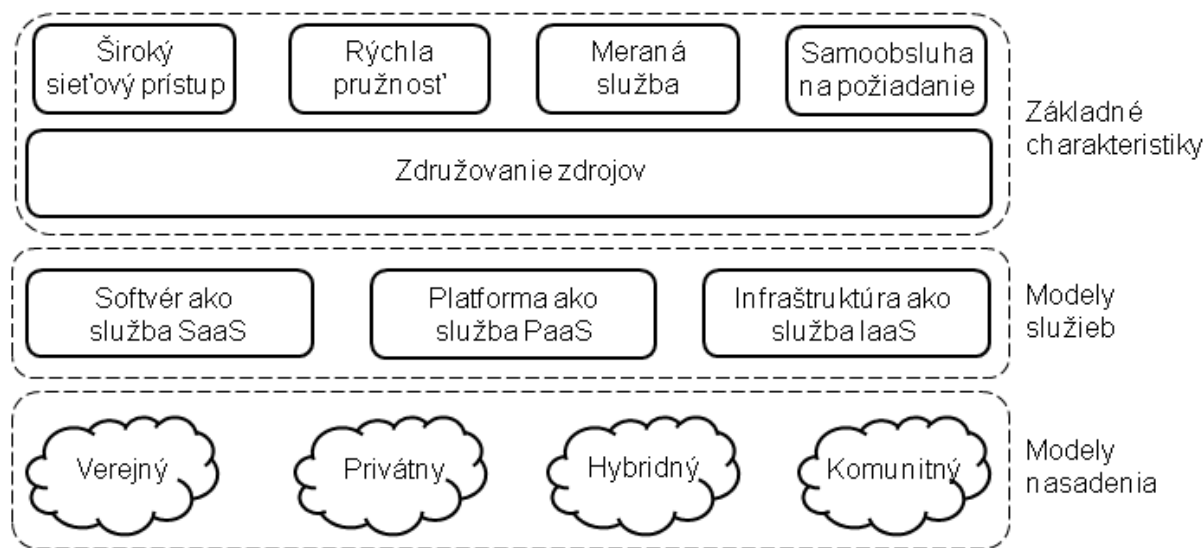
Metodické usmernenie zároveň definuje role, práva a povinnosti zúčastnených strán.

Usmernenie sa zverejňuje na <https://www.mirri.gov.sk/sekcie/certifikacia-a-zapis-sluzieb-vladneho-cloudu/>

## 2 Východiská, terminológia

**Cloudová služba** umožňuje jednoduchý, pohodlný, bezpečný a spoľahlivý sieťový prístup k zdieľanej sade konfigurovateľných výpočtových zdrojov (sieťam, serverom, dátovým úložiskám, aplikáciám, službám ...). Cloud ako taký je progresívna technológia s vysokým potenciálom zlepšenia spolupráce, pružnosti, škálovateľnosti, vysokej dostupnosti, vytvára výrazný priestor na znižovanie nákladov prostredníctvom optimalizácie a efektívneho využívania výpočtových zdrojov. Základné charakteristiky cloudovej služby podľa Amerického národného úradu pre štandardy a technológie NIST (National Institute of Standards and Technology) je možné definovať popisom piatich základných charakteristík, troch modelov cloudových služieb a štyrmi modelmi nasadenia cloudu, ktoré sú zobrazené na nasledovnom obrázku č. 1.

Obrázok č. 1: Základné charakteristiky cloudovej služby



## 2.1 Základné charakteristiky a predpoklady pre využívanie cloudových služieb

Cloudové služby je možné vo všeobecnosti definovať cez ich základné vlastnosti a charakteristiky, ktoré zároveň aj predurčujú oblasť ich efektívneho nasadenia a využívania:

- **širokopásmový sieťový prístup** - funkcie cloudu sú k dispozícii cez sieť (spravidla internet) a prístupné prostredníctvom štandardizovaných mechanizmov, ktoré podporujú používanie heterogénnych platforiem - tenkého alebo tučného klienta (napríklad mobilné telefóny, tablety, notebooky, pracovné stanice ...),
- **rýchla pružnosť (vysoká elasticita)** - kapacita cloudu môže byť elasticky zabezpečovaná a uvoľňovaná v niektorých prípadoch automaticky, vo zvýšenej alebo zníženej miere úmernej dopytu. Zabezpečená dostupná kapacita cloudu sa pre spotrebiteľa môže zdať neobmedzená a môže mu byť poskytnutá kedykoľvek v ľubovoľnom množstve,
- **meraná (merateľná) služba** - cloudové systémy automaticky riadia a optimalizujú využitie dostupných zdrojov s využitím funkcie merania na určitej úrovni abstrakcie zodpovedajúcej typu služby (napríklad pamäť, spracovanie, šírka pásma a aktívne používateľské účty). Používanie zdrojov môže byť monitorované, riadené a oznamované tak, aby sa zabezpečila transparentnosť ako pre poskytovateľa tak aj pre spotrebiteľa využívajúcej služby,
- **samoobsluha na požiadanie** - spotrebiteľ si môže jednostranne zaobstarať výpočtovú kapacitu, ako je čas servera a sieťové úložisko, podľa potreby automaticky bez nevyhnutnosti ľudskej interakcie s každým poskytovateľom služieb,
- **združovanie zdrojov** - výpočtové zdroje poskytovateľa sú združené tak, aby slúžili viacerým spotrebiteľom pomocou modelu viacerých nájomcov, s rôznymi fyzickými a virtuálnymi zdrojmi dynamicky prerozdeľovanými podľa žiadosti spotrebiteľa. Pri prideliťovaní zdrojov existuje princíp nezávislosti umiestnenia v tom, že zákazník vo všeobecnosti nemá žiadnu

kontrolu alebo vedomosť o presnom umiestnení poskytnutých zdrojov, ale môže byť schopný určiť umiestnenie na vyššej úrovni abstrakcie (napríklad štát alebo dátové centrum). Príklady prostriedkov zahŕňajú dátové úložiská, výpočtový výkon, veľkosť operačnej pamäte a šírku pásma siete,

## 2.2 Modely cloudových služieb

Cloudové služby sa <sup>1</sup>rozdeľujú na model:

„**a) infraštruktúra ako služba**, označovaný aj ako **IaaS**, pri ktorom cloudovú službu predstavuje poskytovanie virtualizovanej infraštruktúry ako serverov, úložísk údajov a sieťovej infraštruktúry,

**b) platforma ako služba**, označovaný aj ako **PaaS**, pri ktorom cloudovú službu predstavuje poskytovanie hardvérovej a softvérovej platformy, potrebnej na vytvorenie a správu aplikácií, vrátane umožnenia ich navrhovania, vývoja, testovania a nasadzovania do produkčnej prevádzky, pričom tieto aplikácie ostávajú v správe odberateľa cloudových služieb,

**c) softvér ako služba**, označovaný aj ako **SaaS**, pri ktorom cloudovú službu predstavuje poskytovanie softvéru, vrátane aplikácií.“

Niektoré zdroje uvádzajú aj ďalšie modely cloudových služieb:

- Sieť ako služba – NaaS (Network as a Service),
- Pracovná plocha ako služba – DaaS (Desktop as a Service),
- Diskový priestor ako služba – StaaS (Storage as a Service)
- Riadenie ako služba – MaaS (Management as a Service),
- Obchodný proces ako služba – BPaaS (Business Process as a Service).

## 2.3 Vzťahy a závislosti medzi jednotlivými modelmi cloudových služieb

Model IaaS je základom všetkých cloudových služieb. Ako možno vidieť na nasledovnom obrázku model PaaS je nadstavbou IaaS a SaaS je v poradí ďalšia nadstavba nad PaaS.

**IaaS** obsahuje kompletný zásobník zdrojov infraštruktúry od príslušenstva po hardvérové platformy, ktoré sa v nich nachádzajú. Umožňuje abstrahovať zdroje a poskytovať fyzickú a logickú konektivitu k týmto zdrojom. IaaS poskytuje sadu API, ktoré umožňujú manažment a iné formy interakcie spotrebiteľov s infraštruktúrou.

**PaaS** sedí na vrchole IaaS a pridáva ďalšiu vrstvu integrácie s rámcami vývoja aplikácií, možnosti middleware a funkcie ako je napríklad databáza, zasielanie správ a front. Tieto služby

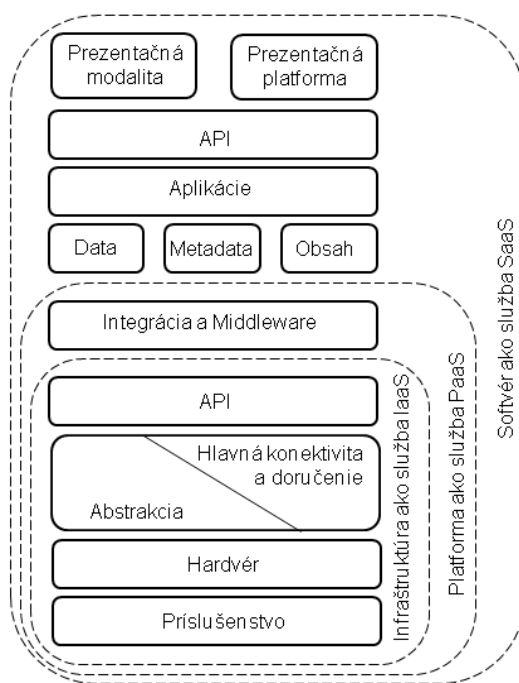
---

<sup>1</sup> § 42 vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z.z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z.

umožňujú vývojárom vytvárať aplikácie na platforme s programovacími jazykmi a nástrojmi, ktoré sú podporované v zásobníku.

**SaaS** je zase postavená na základných zásobníkoch IaaS a PaaS a poskytuje samostatné operačné prostredie, ktoré je využívané na dodanie celej používateľskej praxe, vrátane obsahu, jeho prezentácie, aplikácie/í a možnosti manažmentu.

Obrazok č. 2: Modely cloudových služieb



## 2.4 Modely nasadenia cloudových služieb:

Podľa legislatívy<sup>2</sup> je štandardom pre modely nasadenia cloudových služieb je rozdelenie typov cloudových služieb najmä na:

**a) privátny cloud**, pri ktorom je cloud computing alokovaný výhradne pre potreby jednej organizácie, pričom poskytovateľom cloudových služieb, prevádzkovateľom cloudových služieb ani sprostredkovateľom cloudových služieb nemusí byť táto organizácia,

**b) komunitný cloud**, pri ktorom cloud computing využíva niekoľko organizácií, ktoré tvoria jednu komunitu, zdieľajúcu podobné záujmy, napríklad ciele, požiadavky na bezpečnosť, politiku a dodržiavanie záujmov, pričom poskytovateľom cloudových služieb, prevádzkovateľom cloudových služieb ani sprostredkovateľom cloudových služieb nemusí byť ani jedna z týchto organizácií,

**c) verejný cloud**, pri ktorom je cloud computing zdieľaný ľubovoľnými odberateľmi cloudových služieb, pričom ani jeden z nich nemusí byť poskytovateľom cloudových služieb alebo prevádzkovateľom cloudových služieb,

<sup>2</sup> Vyhláška č. 78/2020 Z. z. § 42

**d) hybridný cloud**, ktorý predstavuje kompozitné využitie cloudových služieb dvoch alebo viacerých modelov cloud computingu, pričom využívané cloudové služby sú naďalej podporované jednotlivými infraštruktúrnymi prostriedkami daných modelov cloud computingu, ale ako také sú vzájomne spojené štandardizovanými alebo proprietárnymi technológiami, ktoré umožňujú prenositeľnosť údajov a aplikácií.“

## 2.5 Kategórie cloudových služieb pre OVM

Cloudové služby, ktoré majú byť uvedené v Katalógu cloudových služieb sa delia na základe bezpečnostných požiadaviek pre uchovávané a spracovávané dáta, pričom bezpečnostné požiadavky sú analyzované a posudzované osobitne z hľadiska dôveryhodnosti, integrity a dostupnosti spracovávaných a uchovávaných dát.

Úroveň miery vplyvu jednotlivých bezpečnostných požiadaviek na uchovávané a spracovávané dáta je nasledovná:

- Žiadna
- Nízka
- Stredná
- Vysoká
- **Kritická**

Požiadavky na bezpečnostnú úroveň sú uvedené v tabuľke č. 1.

Všeobecné vyjadrenie bezpečnostnej úrovne informácie má tvar:

**C(0, 1, 2, 3), I(0, 1, 2, 3), A(0, 1, 2, 3).**

Tabuľka č. 1: Požiadavky na bezpečnostnú úroveň poskytovateľa služby

| Bezpečnostná požiadavka  | Žiadna (0)                                         | Nízka (1)                                                                                                         | Stredná (2)                                                                                                     | Vysoká (3)                                                                                                               |
|--------------------------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <b>Dôveryhodnosť (C)</b> | Neexistuje požiadavka na dôveryhodnosť informácie. | Neautorizované zverejnenie informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.                | Neautorizované zverejnenie informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.                | Neautorizované zverejnenie informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.                |
| <b>Integrita (I)</b>     | Neexistuje požiadavka na integritu informácie.     | Neautorizované modifikácia alebo zničenie informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby. | Neautorizované modifikácia alebo zničenie informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby. | Neautorizované modifikácia alebo zničenie informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby. |
| <b>Dostupnosť (A)</b>    | Neexistuje požiadavka na dostupnosť informácie.    | Nedostupnosť informácie môže mať obmedzený vplyv na procesy, služby, aktíva a osoby.                              | Nedostupnosť informácie môže mať závažný vplyv na procesy, služby, aktíva a osoby.                              | Nedostupnosť informácie môže mať obzvlášť závažný vplyv na procesy, služby, aktíva a osoby.                              |

|  |    |          |                |
|--|----|----------|----------------|
|  | U4 | Kritická | Privátny cloud |
|  | U3 | Vysoká   | Verejný cloud  |
|  | U2 | Stredná  | Verejný cloud  |
|  | U1 | Nízka    | Verejný cloud  |

Ďalšie informácie k úrovniam cloudových služieb sú v dokumente:

## 1K\_Urovne\_cloudovych\_sluzieb\_na\_zapis\_CS

Podľa požiadaviek na bezpečnostnú úroveň spracovávaných údajov a podľa účelu a spôsobu ich spracovávaní sa cloudové služby delia na nasledovné kategórie:

**Kategória U1: Verejné - Open Data (Základná úroveň zabezpečenia)** - dáta, ktoré sú verejne dostupné a použiteľné. V prípade poskytovania infraštruktúry na vývoj IS sa dáta považujú za open data. Za Open data podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C0I0A0 a C0I0A1. Pre zaradenie ponúkanej cloudovej služby do kategórie U1 je určený postup formou samohodnotenia poskytovateľom cloudovej služby.

*Úroveň pre spôsob hodnotenia: C0I0A0 a C0I1A1*

**Kategória U2: Dôverné dáta (Stredná úroveň zabezpečenia)** - dáta potrebné pre fungovanie IS VS (napr. neštruktúrované informácie potrebné k vyriešeniu životnej situácie občana, štruktúrované informácie potrebné k vyriešeniu životnej situácie občana). Za Dôverné dáta podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C1I1A1 až C1I1A2. Pre zaradenie ponúkanej cloudovej služby do kategórie U2 je určený postup posúdenia a ohodnotenia ponúkanej cloudovej služby kvalifikovaným hodnotiteľom (viď **Chyba! Nenašiel sa žiaden zdroj odkazov. Chyba! Nenašiel sa žiaden zdroj odkazov.**).

*Úroveň pre spôsob hodnotenia: C1I2A2 až C2I2A2*

**Kategória U3: Regulované dáta (Vysoká úroveň zabezpečenia)** – dáta, nakladanie s ktorými je upravené osobitnými právnymi predpismi. Za Regulované dáta podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C2I1A1 až C3I3A3.

Pre zaradenie ponúkanej cloudovej služby do kategórie U3 je určený postup posúdenia a ohodnotenia ponúkanej cloudovej služby certifikovaným Audítorom kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len “zákon č. 69/2018 Z. z.”).

*Úroveň pre spôsob hodnotenia: C3I3A3*

**Kategória U4: Špeciálne dáta (Kritická úroveň zabezpečenia)** – sú dáta s ktorými nakladanie je upravené osobitnými právnymi predpismi. Za **špeciálne** dáta podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C3I3A3, ktoré však vyžadujú uchovávanie a spracovávanie dát na území SR a v dátovom centre, ktoré je v dosahu štátnych orgánov SR, v **privátnej časti vládneho cloudu**.

Pre zaradenie ponúkanej cloudovej služby do kategórie **U4** je určený postup posúdenia a ohodnotenia ponúkanej cloudovej služby certifikovaným Audítorom kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z..

*Úroveň pre spôsob hodnotenia: C3I3A3 a zároveň umiestnenie údajov a ich spracovanie na území SR.*

## 2.6 Doba platnosti hodnotenia poskytovanej cloudovej služby

Doba platnosti zápisu cloudovej služby **kategórie U1, U2, U3 a U4** do Katalógu ponúkaných cloudových služieb je **2 roky** od dátumu zápisu.

Poskytovateľ cloudovej služby môže požiadať o predĺženie zápisu v zozname cloudových služieb najskôr 6 mesiacov pred uplynutím 2 ročnej platnosti zápisu, avšak najneskôr 60 kalendárnych dní pred uplynutím platnosti zápisu (na nové hodnotenie cloudovej služby má 60 kalendárnych dní).

V prípade, ak poskytovateľ cloudovej služby nevykoná (*neaktualizuje*) nové ohodnotenie v stanovenej lehote, alebo hodnotiaci proces ponúkanej cloudovej služby nebude do tejto doby úspešný, cloudová služba bude z katalógu cloudových služieb automaticky vymazaná. V prípade vymazania cloudovej služby musia poskytovateľ a prevádzkovateľ cloudovej služby poskytnúť dostatočnú dobu na presun informačných systémov k inému prevádzkovateľovi CS.

## 2.7 Úloha a postavenie MIRRI

V procese zaraďovania ponúkanej cloudovej služby do katalógu má MIRRI úlohu jednak koordinátora celého procesu, jeho metodické usmerňovanie a zabezpečuje prevádzku katalógu ponúkaných vládnych cloudových služieb.

## 2.8 Používateľ ponúkanej cloudovej služby

Ponúkaná cloudová služba zaradená do katalógu je určená pre používateľov, ktorými sú primárne OR. Výber ponúkanej cloudovej služby z katalógu poskytne OR záruku, že vybraná cloudová služba podľa zvolenej kategórie (U1, U2, U3, U4) spĺňa príslušné kvalitatívne a bezpečnostné kritériá.

Po výbere vládnej cloudovej služby z katalógu má OR oznamovaciu povinnosť zaevidovať používanie cloudovej služby k ISVS do MetaIS.

V prípade, ak OR zakomponuje vládnu cloudovú službu do svojej infraštruktúry, musí celá infraštruktúra zodpovedať bezpečnostným požiadavkám na ISVS (zodpovednosť OR), definovanými v zákone č. 69/2018 Z.z. .

## 2.9 Poskytovateľ ponúkanej cloudovej služby

**Poskytovateľ ponúkanej cloudovej služby** je osoba, ktorá je zodpovedná za správu cloud computingu a poskytovanie cloudových služieb, poskytuje definovanú cloudovú službu (**IaaS**,

**Paas, SaaS ...)** orgánom riadenia, a to podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb a na základe zmluvného vzťahu s prevádzkovateľom cloudovej služby.

**Poskytovateľ cloudovej služby** je oprávnený byť poskytovateľom „**Podpory ako Služby**“<sup>3)</sup>

## 2.10 Prevádzkovateľ ponúkanej cloudovej služby

Prevádzkovateľom cloudových služieb je osoba, ktorá na základe zmluvného vzťahu s poskytovateľom cloudových služieb zabezpečuje technické podmienky na prevádzkovanie, prepojenie a prenos cloudových služieb.

Prevádzkovateľ cloudovej služby nemusí byť priamo vlastníkom a správcom celej infraštruktúry dátových centier, výkon jednotlivých častí poskytovanej služby môže byť realizovaný aj subdodávateľskou formou, táto štruktúra však musí byť transparentná, preukázateľná a auditovateľná.

Prevádzkovateľ cloudovej služby zároveň môže ale nemusí byť priamo subjektom, ktorý sprostredkováva (poskytuje) ponúkanú cloudovú službu koncovým používateľom. Takýmto subjektom môže byť napr. zmluvný partner Prevádzkovateľa ponúkanej cloudovej služby alebo broker.

Prevádzkovateľ cloudovej služby, ktorý je aj subjektom, ktorý poskytuje ponúkané cloudové služby koncovým používateľom, stáva sa zároveň poskytovateľom cloudovej služby.

## 2.11 Sprostredkovateľ cloudovej služby

Sprostredkovateľ cloudovej služby je osoba, ktorá na základe zmluvného vzťahu s poskytovateľom, v ojedinelých prípadoch s prevádzkovateľom cloudových služieb prevádzkuje využívanie, výkon a dodávku cloudových služieb tretím stranám podľa podmienok dohodnutých v dohode o poskytovanej úrovni cloudových služieb.

Sprostredkovateľ cloudovej služby **nesmie** byť poskytovateľom „**Podpory ako Služby**“, a z toho dôvodu nie je povinný požiadať o zápis tých služieb do KsVC, ktoré sprostredkováva.

## 2.12 Poskytovateľ podpory ako služby

Poskytovateľom podpory ako služby je osoba, ktorá je na základe zmluvného vzťahu s odberateľom cloudových služieb zodpovedná za poskytovanie technickej a personálnej podpory pri správe a implementácii infraštruktúrnych komponentov, platformových komponentov alebo softvérových komponentov alebo iných systémov, softvérov a zariadení v oblasti cloud computingu.

---

<sup>3</sup> § 41 písm. i) vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z.z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z.

Poskytovateľ podpory ako služby, je **povinný** požiadať o zápis tých služieb do KsVC, pre ktoré poskytuje službu „Podpora ako služba“<sup>4</sup>.

Podporou ako službou sa rozumie poskytovanie technickej a personálnej podpory pri správe a implementácii infraštruktúrnych komponentov, platformových komponentov alebo softvérových komponentov alebo iných systémov, softvérov a zariadení v oblasti cloud computingu.

## 3 Životný cyklus cloudovej služby

### 3.1 Žiadosť o zápis ponúkanej cloudovej služby do KsVC

Poskytovateľ alebo prevádzkovateľ ponúkanej cloudovej služby je povinný podľa zákona podať na MIRRI **žiadosť o zaradenie** (príloha 1A\_Žiadosť o registráciu CS) ním poskytovanej cloudovej do Katalógu cloudových služieb.

Poskytovateľ alebo prevádzkovateľ ponúkanej cloudovej služby podáva žiadosť o zaradenie :

- **cloudovej služby** – ktorá sa skladá z jedinej služby v cloude,

Formulár žiadosti o zaradenie ponúkanej cloudovej služby do Katalógu cloudových služieb je umiestnený na webovom sídle <https://www.mirri.gov.sk/sekcie/certifikacia-a-zapis-sluzieb-vladneho-cloudu/>

Žiadosť obsahuje **identifikačné údaje** poskytovateľa cloudovej služby, **prevádzkovateľa** cloudovej služby a **opis** cloudovej služby (charakteristiku ponúkanej cloudovej služby a jej základné parametre).

Pre preukázanie kvality a vyspelosti cloudovej služby, záujemca môže doložiť platné certifikáty pokrývajúce príslušné časti hodnotenia v katalógu vlastností cloudových služieb (prílohy **1C\_Katalóg vlastností CS**, **1I\_Poziadavky\_na\_zapis\_CS**).

V žiadosti musí uviesť príslušnú úroveň ponúkanej služby (U1, U2, U3, U4), od ktorej bude závisieť spôsob hodnotenia ponúkanej služby.

*Povinnou súčasťou žiadosti sú obchodné podmienky poskytovateľa cloudovej služby, vzor zmluvy medzi používateľom a poskytovateľom ponúkanej cloudovej služby a zmluva o úrovni poskytovaných služieb (Service Level Agreement, ďalej len SLA).*

V zmluve SLA musia byť uvedené merateľné parametre ponúkanej služby, ktoré budú slúžiť nielen ako kritérium posudzovanej a ohodnocovanej služby, ale aj pri následnom monitorovaní a kontrole parametrov poskytovanej služby počas jej doby poskytovania.

Ak má poskytovateľ svojich subdodávateľov (napr. poskytovateľ služieb vzdialeného záložného dátového centra), je povinný v žiadosti uviesť zoznam všetkých subdodávateľov aj s uvedením ich sídel a zároveň zoznam všetkých lokalít dátových centier kde sú ukladané dáta (čo je dôležité napr. pri uchovávaní osobných údajov mimo EÚ).

---

<sup>4</sup> vyhláška ÚPVII 78/2020 Z. z. o štandardoch pre informačné technológie verejnej správy, § 41, odstavce i, j

Keďže každá jedna ponúkaná cloudová služba je posudzovaná a hodnotená samostatne, pre každú jednotlivú ponúkanú cloudovú službu je nutná individuálna žiadosť.

Po vyhodnotení formálnych náležitostí a posúdení žiadosti (kontrola žiadosti a jej príloh po stránke formálnej) MIRRI rozhodne, či posudzovaná žiadosť bude zaradená do príslušného hodnotiaceho procesu v závislosti od príslušnej kategórie ponúkanej služby.

Následne žiadateľ **musí preukázať, že cloudová služba spĺňa štandardy poskytovania cloud computingu a využívania cloudových služieb podľa štandardov informačných systémov verejnej správy podľa príslušnej kategórie U1, U2, U3 alebo U4.**

Popis požadovaných informácií a dokladov je v prílohách:

- **1G\_Popis\_procesov** a
- **1I\_Poziadavky\_na\_zapis\_CS**

### 3.1.1 Rozdelenie ponúkaných cloudových služieb do jednotlivých kategórií

Ponúkané cloudové služby podľa obsahu a úrovne parametrov (C, I ,A) spracovávaných údajov sa delia na nasledovné kategórie U1,U2,U3,U4. Pre každú z uvedených kategórií je nutná osobitná forma posúdenia a ohodnotenia poskytovateľa a samotnej cloudovej služby.

#### 3.1.1.1 Kategória U1

Najmenej citlivou a najmenej kritickou je **kategória U1**, tzv. Open Data (Základná úroveň zabezpečenia). Ponúkaná cloudová služba spracováva a narába s dátami, ktoré sú verejne dostupné a použiteľné. Za Open data podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C0I0A0 a C0I1A1.

Pre zaradenie ponúkanej cloudovej služby do kategórie U1 je určený postup formou samohodnotenia poskytovateľom cloudovej služby.

Pre účely posudzovania kvality a vyspelosti cloudovej služby považujeme vývojové a testovacie prostredie za prostredie kategórie U1 za predpokladu, že nebude obsahovať reálne údaje a nebude na ňom služba produkčne prevádzkovaná.

#### 3.1.1.2 Kategória U2

Spracovávané dáta zo **Strednou mierou citlivosti** sú zaradené do **kategórie U2 (Stredná úroveň zabezpečenia)** - dáta potrebné pre fungovanie IS VS (napr. neštruktúrované informácie potrebné k vyriešeniu životnej situácie občana, štruktúrované informácie potrebné k vyriešeniu životnej situácie občana).

Za dáta, ktoré sú s vyššou mierou citlivosti zaradené do kategórie U2, podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C1I2A2 až C1I2A2.

*Pre zaradenie ponúkanej cloudovej služby do kategórie U2 je určený postup posúdenia a ohodnotenia ponúkanej cloudovej služby hodnotiteľom MIRRI.*

### 3.1.1.3 Kategória U3

**Vysoko citlivé dáta** a ich spracovávanie formou ponúkanej cloudovej služby sú zaradené do **kategórie U3 (Vysoká úroveň zabezpečenia)**, čo sú dáta, s ktorými nakladanie je upravené osobitnými právnymi predpismi. Za Regulované dáta podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C3I3A3.

Pre zaradenie ponúkanej cloudovej služby do kategórie U3 je určený postup posúdenia a ohodnotenia ponúkanej cloudovej služby certifikovaným Audítorm kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z.

### 3.1.1.4 Kategória U4

Kritické dáta a ich spracovávanie formou ponúkanej cloudovej služby sú zaradené do **kategórie U4 (Kritická úroveň zabezpečenia)**, čo sú dáta, s ktorými nakladanie je upravené osobitnými právnymi predpismi a zároveň vyžadujú uchovávanie a spracovávanie v privátnej časti vládneho cloudu. Za Kritické dáta podľa vyššie uvedených bezpečnostných požiadaviek sa považujú uchovávané a spracovávané dáta úrovne C3I3A3 a zároveň existuje oprávnený záujem, aby pôsobnosť nad týmito dátami mala výhradne Slovenská republika.

*Pre zaradenie ponúkanej cloudovej služby do kategórie U4 je určený postup posúdenia a ohodnotenia ponúkanej cloudovej služby certifikovaným Audítorm kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z.*

## 3.1.2 Uznávanie certifikácií tretích strán

Cieľom uznávania certifikácií cloudových služieb tretích strán je minimalizácia zaťaženia poskytovateľov cloudových služieb pri získavaní akreditácie služby vládneho cloudu. Akonáhle už poskytovateľ získal certifikáciu "X", nie je potrebné kompletne overovať pri certifikácii „Y“ akreditácie. Účelom je preto podporovať spoluprácu medzi rôznymi bezpečnostnými rámcami, normami a najlepšími postupmi.

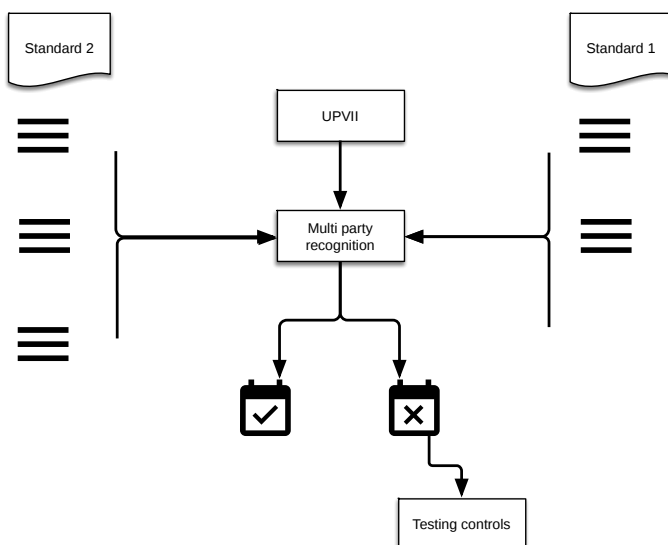
Ak záujemca o evidenciu cloudovej služby v katalógu je držiteľom niektorého z medzinárodných certifikátov, primárne orientovaných na bezpečné a spoľahlivé prevádzkovanie aplikácií a služieb v prostredí cloudu, svoju spôsobilosť alebo kvalifikáciu pre určitú oblasť preverovaných skutočností uvedie do formulára (príloha 1B prípadne 1C) vo forme odkazu na príslušný platný certifikát, ktorý bol predložený k registrácii<sup>5</sup>. Vzhľadom na fakt, že spoločnosti využívajú rôzne certifikačné schémy kvality a bezpečnosti cloudových služieb, MIRRI posúdi pre účely hodnotenia splnenie alebo nesplnenie kritéria v katalógu a nie je potrebné znova overovať službu, a zvyšovať tak náklady spojené s overovaním parametrov cloudových služieb.

V mnohých prípadoch by sa práca vykonaná v rámci jednej certifikácie mala opätovne použiť v rámci inej certifikácie služby, čo poskytovateľom umožní zamerať sa skôr na rozdiely medzi týmito dvoma certifikačnými schémami.

---

<sup>5</sup> <https://resilience.enisa.europa.eu/cloud-computing-certification/>

Obrázok č. 3: Multiparty recognition



### Ilustračný príklad:

1. Poskytovateľ, ktorý je držiteľom certifikátu napr. CSA STAR, požiada MIRRI o overenie služby.
2. MIRRI na základe vyhodnotenia predloženej certifikácie stanoví minimálny rozsah kontrolných otázok.

Poskytovateľ môže v odpovedi na kontrolné otázky uviesť odkaz na príslušný platný certifikát, ktorý bol predložený k registrácii. Poskytovateľ sa môže zamerať na opis toho, ktoré kontrolné ciele nie sú pokryté CSA STAR.

### 3.1.3 Preukázanie kvalifikácie pre poskytovanie služby

Záujemca o poskytovanie cloudových služieb je povinný v žiadosti o zaradenie ponúkanej cloudovej služby do Katalógu poskytovaných cloudových služieb preukázať svoju kvalifikovanosť poskytovať ponúkanú cloudovú službu príslušnej kategórie (U1, U2, U3, U4).

Pre poskytovanie cloudových služieb **kategórie U1** záujemca nie je povinný dokladovať svoju kvalifikáciu pre poskytovanie cloudových služieb špecifickými certifikátmi.

Pri cloudových službách **kategórie U2** je potrebné doložiť certifikáty ktoré sú povinné, prípadne je možné doložiť ďalšie certifikáty, ktoré pokrývajú jednotlivé oblasti hodnotenia napr. pre všeobecnú úroveň kvality poskytovania služieb postačuje certifikát systému manažérstva kvality na úrovni ISO9001:2015. Uchádzač musí byť držiteľom certifikátu typu ISO 27001 (27017, 27018) alebo ekvivalentného certifikátu, túto časť je možné akceptovať ako súčasť príslušného hodnotenia.

**Kategória U3** si vyžaduje rovnaké požiadavky ako U2 a zároveň dodanie špecifických, primárne bezpečnostných certifikátov, resp. bezpečnostné preverky na príslušnú úroveň. Bližšie informácie v prílohách **1C\_Katalóg vlastností CS**, **1I\_Poziadavky\_na\_zapis\_CS**.

**Kategória U4** si vyžaduje rovnaké požiadavky ako U3 a zároveň absolvovanie Auditú KB podľa zákona č. 69/2018 Z. z. s dosiahnutím súladu s požiadavkami minimálne **90%?**

Pre preukázanie kvalifikačných predpokladov pre služby kategórie U2, U3, U4 postačuje priloženie kópií jednotlivých certifikátov a ich auditných správ v elektronickej podobe.

MIRRI, alebo používateľ/OR si môže preveriť informácie uvedené v hodnotiacom formulári formou auditu (U1, U2, U3, U4).

**Všetky požiadavky (požadované a doporučované) pre jednotlivé kategórie sú v dokumente „1I\_Poziadavky\_na\_zapis\_CS“ v tabuľke č.1.**

## 3.2 Proces hodnotenia služby

### 3.2.1 Hodnotiteľ

Podmienkou pre zaradenie ponúkanej cloudovej služby do kategórie U1 a U2 je posúdenie a ohodnotenie tejto služby hodnotiteľom. Hodnotiteľom môže byť osoba, ktorá má príslušné kvalifikačné predpoklady pre túto činnosť. Bližší popis Hodnotiteľa a jeho požadované kvalifikačné predpoklady sú bližšie špecifikované v dokumente „1E\_Popis hodnotiteľa CS“. Hodnotiteľom môže byť aj zamestnanec MIRRI.

Podmienkou pre zaradenie ponúkanej cloudovej služby do kategórie U3, U4 je posúdenie a ohodnotenie tejto služby nezávislou a spôsobilou osobou – hodnotiteľom, ktorým môže byť výlučne certifikovaný Audítor kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. .

### 3.2.2 Pôsobnosť hodnotiteľa pre jednotlivé kategórie ponúkanej CS.

Kategória ponúkanej cloudovej služby **U1 nevyžaduje hodnotiteľa**, nakoľko pre túto kategóriu cloudovej služby vyplňa požadovaný dotazník samotný záujemca o poskytovanie ponúkanej cloudovej služby. MIRRI v tomto prípade vykonáva funkciu kontrolného a dohliadajúceho orgánu s právomocou preverovať skutočnosti, uvedené v dotazníku (príloha **1B\_Formulár pre samohodnotenie CS**).

Pre posúdenie ponúkanej cloudovej služby **kategórie U2, U3 a U4** je funkcia hodnotiteľa nutná. Samotný proces posudzovania cloudovej služby vykonáva:

- kategória U2 vykonáva priamo hodnotiteľ MIRRI,
- kategória U3 a U4 vykonáva certifikovaný Audítor kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z.

Ak to rozsah hodnotenej cloudovej služby vyžaduje, MIRRI môže určiť aj viacero hodnotiteľov.

Hodnotiteľov **kategórie U2** vyberá a akredituje priamo MIRRI, pričom MIRRI zároveň vykonáva priamy dohľad nad hodnotiteľmi.

Hodnotenie služby **kategórie U3, U4** je vykonané certifikovanými Audítormi kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. , ktorých zabezpečí MIRRI v súčinnosti s NBÚ.

Hodnotiteľ pri hodnotení označí splnenie požadovaných požiadaviek a dodaných súčastí žiadosti v kontrolnom formulári hodnotiteľa v dokumente **1J\_Hodnotenie-hodnotiteľom**

Bližší popis hodnotiteľa je v prílohe **1E\_Hodnotiteľ CS**.

### 3.2.3 Formulár pre samohodnotenie pre kategóriu U1

Pre poskytovanie cloudovej služby pre OVM kategórie U1 záujemca o zápis cloudovej služby vyplní dotazník pre samohodnotenie (príloha 1B\_Formulár pre samohodnotenie CS). Dotazník je dostupný na webovom sídle MIRRI: <https://www.mirri.gov.sk/sekcie/certifikacia-a-zapis-sluzieb-vladneho-cloudu/>, a sú k dispozícii pre každého záujemcu.

Dotazník je vo formáte \*.xlsx, uchádzač bude požadované údaje zapisovať do vymedzených riadkov tabuľky. Za správnosť uvedených údajov nesie zodpovednosť záujemca.

Ak záujemca má dokumenty, ktoré majú slúžiť ako prílohy k dotazníku (aj v prípade ak poskytovateľ je držiteľom niektorého z medzinárodných certifikátov podľa kapitoly **Chyba! Nenašiel sa žiaden zdroj odkazov..** Uznávanie certifikácií tretích strán – multiparty recognition) priloží ich v elektronickej podobe (napr. naskenované listinné dokumenty).

Nie je nutné prikladať originály dokumentov (napr. odborné certifikáty), v prípade ak sa MIRRI rozhodne niektoré skutočnosti, uvedené v dotazníku preveriť, záujemca je povinný predložiť MIRRI originály dokumentov.

#### Vypĺňanie formulára

1. V prvej časti dotazníku pre samohodnotenie záujemca uvedie základné údaje o poskytovateľovi ponúkanej cloudovej služby. Uvedené údaje sa musia zhodovať s údajmi z príslušných relevantných registrov (obchodný register, živnostenský register alebo ekvivalentné registrové databázy v prípade ak záujemca nepôsobí priamo na území SR). Uvedené údaje by mali byť preukázateľné a overiteľné. Táto časť dotazníka je dôležitá pre transparentnosť a boj proti korupcii a klientelizmu (súlady s platnými právnymi predpismi). Zároveň je potrebné uviesť okolnosti možného prístupu tretích strán (technický a prevádzkový personál) a úroveň legislatívnych obmedzení (regulácia).
2. V druhej časti dotazníka, tá sa týka profilu samotnej spoločnosti ako poskytovateľa cloudovej služby, kde záujemca uvedie počet pracovníkov priamo zapojených do oblasti poskytovania cloudových služieb, celkový počet zamestnancov spoločnosti a časové obdobie svojho pôsobenia na trhu cloudových služieb.
3. Tretia časť dotazníka sa týka základných informácií o samotnej službe. Záujemca do dotazníka uvedie údaje, ako sú názov služby, stručný popis služby, celkový počet prevádzkovaných cloudových služieb a adresu webového sídla s bližším popisom cloudovej služby. Záujemca v dotazníku uvedie popis uplatnenia ponúkanej služby na trhu formou uvedenia počtu ako zákazníkov, tak aj celkového počtu používateľov. V závere tejto časti dotazníka záujemca uvedie ním vlastnené certifikáty a osvedčenia z oblasti technickej, z oblasti riadenia kvality, súladu a zhody, z oblasti ochrany a bezpečnosti dát ako aj odvetvovo špecifické certifikáty. K dotazníku prikladá záujemca kópiu certifikátu alebo osvedčenia. Do dotazníka záujemca uvedie názov a typ osvedčenia spolu s dobou jeho platnosti. Tie isté údaje uvedie záujemca aj pre certifikáty a osvedčenia subdodávateľov alebo prevádzkovateľov dátových centier.

Záujemca v dotazníku uvedie základné zmluvné podmienky, podmienky zrušenia zmluvy, informácie o lokalizácii uchovávaných dát, podmienky prístupu klienta k dátam, základné

parametre SLA a ceny a nákladové položky za poskytované služby. Tieto slúžia ako vstup pre zhodnotenie korektnosti a transparentnosti zmluvných podmienok.

V dotazníku záujemca zdokumentuje a uvedie prevádzkové aspekty ponúkanej cloudovej služby. Je potrebné uviesť minimálne požiadavky na správu a prevádzku dátového centra a príslušných zariadení, informácie o kontrole prístupov, podmienkach bezpečnej prevádzky, organizácii dátového centra, údaje o službách podpory, popis manažmentu problémových stavov, riadenia zmien, kapacitného plánovania, riadenia dostupnosti služieb a správy zálohovania.

V rámci zmluvného zabezpečenia je dôležité zabezpečiť dodržiavanie autorských práv a vymedzenie práv na používanie produktov duševného vlastníctva (vendor lock-in<sup>6</sup>). V dotazníku záujemca uvedie, či je zákazník odškodnený pri nedodržaní podmienok používania služby treťou stranou, podmienky, za akých sa ukončí poskytovanie zmluvnej podpory pri skončení platnosti zmluvy a či sú definované zmluvné pravidlá a opatrenia pre pomoc zákazníčkovi v prípade ukončenia zmluvného poskytovania služby.

4. Rozhodujúcim parametrom pri poskytovaní služieb umiestnených v cloude je otázka bezpečnosti. Zabezpečenie dát a súvisiacich procesov musí záujemca v dotazníku popísať vo forme zásad riadenia bezpečnosti, či je zabezpečené efektívne riadenie bezpečnosti informácií ISMS (ISO 27001 apod.) a uviesť mieru súladu bezpečnostnej architektúry služby s dokumentom "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti"<sup>7</sup>, mieru vzdelávania personálu v oblasti bezpečnosti, popísať oblasť nácvikov riešenia krízových situácií, uviesť podrobnosti o technickom zabezpečení dátových centier, uviesť informácie o riadení prístupov a správe hesiel ako aj mieru ochrany uchovávaných údajov šifrovaním.
5. V záverečnej časti dotazníka záujemca zodpovie špecifické otázky ohľadom prístupu hypervízora (dvojfaktorová autentifikácia pre prístup k samoobslužným službám, existencia užívateľských smerníc na zaistenie bezpečnosti virtuálnych strojov), izolovaniu jednotlivých aplikácií (úroveň izolovanosti a jej otestovanie), bezpečnostných technológií a operačných systémov (či sú bezpečnostné opatrenia primerané ponúkanej technológii, či je zaručená primeraná webová a aplikačná bezpečnosť, či sú všetky poskytované systémy licenčne vysporiadané a či je technológia dôsledne zdokumentovaná), formátov pre výmenu dát (či existuje dokumentácia ohľadom exportných a importných formátov a či je zaručená v exporte celá referenčná integrita vrátane prístupových oprávnení) a či existuje užívateľská dokumentácia..

### 3.2.4 Dotazníkový formulár pre hodnotenie pre kategóriu U2, U3, U4

Pre poskytovanie cloudovej služby pre OR kategórie U2, U3, U4 vyplní záujemca formuláre pre hodnotenie prílohy:

- 1C\_Formulár\_pre\_hodnotenie\_CS

---

<sup>6</sup> [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=2327](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2327)

<sup>7</sup> <https://www.csirt.gov.sk/metodika-zabezpecenia-ikt.html>

- 1F\_Mapovanie\_Pracovna\_Príloha.

Dotazníky budú dostupné na webovom sídle MIRRI

<https://www.mirri.gov.sk/sekcie/certifikacia-a-zapis-sluzieb-vladneho-cloudu/>

a budú k dispozícii pre každého záujemcu.

Dotazníky sú vo formáte \*.xlsx, \*.docx uchádzač bude požadované údaje zapisovať do vymedzených riadkov tabuľky.

### **Za správnosť uvedených údajov nesie zodpovednosť záujemca.**

Ak záujemca má dokumenty, ktoré majú slúžiť ako prílohy k dotazníku (aj v prípade ak poskytovateľ je držiteľom niektorého z medzinárodných certifikátov podľa kapitoly **Chyba! Nenašiel sa žiaden zdroj odkazov..** Uznávanie certifikácií tretích strán – multiparty recognition) priloží ich v elektronickej podobe (napr. naskenované listinné dokumenty).

Nie je nutné prikladať originály dokumentov (napr. odborné certifikáty), v prípade ak sa MIRRI rozhodne niektoré skutočnosti, uvedené v dotazníku preveriť, záujemca je povinný predložiť koordináčnemu orgánu originály dokumentov.

Vypĺňanie formulára sa vykonáva princípom Otázka -> Odpoveď -> Dôkaz

1. V úvodnej časti dotazníka pre samohodnotenie záujemca uvedie základné údaje o sebe ako poskytovateľovi ponúkanej cloudovej služby. Uvedené údaje sa musia zhodovať s údajmi z príslušných relevantných registrov (obchodný register, živnostenský register alebo ekvivalentné registrové databázy v prípade ak záujemca nepôsobí priamo na území SR). Uvedené údaje by mali byť preukázateľné a overiteľné. Záujemca v prvej všeobecnej časti vyplní základné údaje o poskytovateľovi cloudovej služby, ako je názov spoločnosti, právna forma, IČO, DIČ (alebo ekvivalentný registračný údaj), adresu sídla spoločnosti, adresu webového sídla spoločnosti, štatutárov spoločnosti, kontaktné údaje na zodpovedné osoby, úplné kontaktné údaje primárneho a sekundárneho (záložného) dátového centra, ich názvy a adresy ako aj ich vlastnícku štruktúru. Táto časť dotazníka je dôležitá pre transparentnosť a boj proti korupcii a klientelizmu (súladi s platnými právnymi predpismi). Zároveň je potrebné uviesť okolnosti možného prístupu tretích strán (technický a prevádzkový personál) a úroveň legislatívnych obmedzení (regulácia).
2. V druhej časti dotazníka, tá sa týka profilu samotnej spoločnosti ako poskytovateľa cloudovej služby, kde záujemca uvedie počet pracovníkov priamo zapojených do oblasti poskytovania cloudových služieb, celkový počet zamestnancov spoločnosti a časové obdobie svojho pôsobenia na trhu cloudových služieb.
3. Tretia časť dotazníka sa týka základných informácií o samotnej službe. Záujemca do dotazníka uvedie údaje, ako sú názov služby, stručný popis služby, celkový počet prevádzkovaných cloudových služieb a adresu jej webového sídla. Záujemca v dotazníku uvedie popis uplatnenia ponúkanej služby na trhu formou uvedenia počtu ako zákazníkov, tak aj celkového počtu používateľov. V závere tejto časti dotazníka záujemca uvedie ním vlastnené certifikáty a osvedčenia z oblasti technickej, z oblasti riadenia kvality, súladu a zhody, z oblasti ochrany a bezpečnosti dát ako aj odvetvovo špecifické certifikáty. K dotazníku prikladá záujemca kópiu certifikátu alebo osvedčenia.

Do dotazníka záujemca uvedie názov a typ osvedčenia spolu s dobou jeho platnosti. Tie isté údaje uvedie záujemca aj pre certifikáty a osvedčenia subdodávateľov alebo prevádzkovateľov dátových centier.

Základom korektného vzťahu medzi poskytovateľom a prijímateľom služby sú dobre postavené zmluvné vzťahy. Zmluva musí byť transparentná a výhodná pre obe strany. V dotazníku pre samohodnotenie je zmluvným vzťahom vyhradená dôležitá časť. Záujemca v dotazníku uvedie základné zmluvné podmienky, podmienky zrušenia zmluvy, informácie o lokalizácii uchovávaných dát, podmienky prístupu klienta k dátam, základné aspekty SLA a ceny a nákladové položky za poskytované služby.

V dotazníku záujemca zdokumentuje a uvedie prevádzkové aspekty ponúkanej cloudovej služby. Je potrebné uviesť minimálne požiadavky na správu a prevádzku dátového centra a príslušných zariadení, informácie o kontrole prístupov, podmienkach bezpečnej prevádzky, organizácii dátového centra, údaje o službách podpory, popis manažmentu problémových stavov, riadenia zmien, kapacitného plánovania, riadenia dostupnosti služieb a správy zálohovania.

V rámci zmluvného zabezpečenia je dôležité zabezpečiť dodržiavanie autorských práv a vymedzenie práv na používanie produktov duševného vlastníctva (vendor lock-in<sup>8</sup>). V dotazníku záujemca uvedie, či je zákazník odškodnený pri nedodržaní podmienok používania služby treťou stranou, podmienky, za akých sa ukončí poskytovanie zmluvnej podpory pri skončení platnosti zmluvy a či sú definované zmluvné pravidlá a opatrenia pre pomoc zákazníkovi v prípade ukončenia zmluvného poskytovania služby.

Rozhodujúcim parametrom pri poskytovaní služieb umiestnených v cloude je otázka bezpečnosti. Zabezpečenie dát a súvisiacich procesov, zabezpečenie efektívneho riadenia bezpečnosti informácií ISMS musí záujemca v dotazníku deklarovať popisne a formou dodania platných certifikátu (ISO 27001, s vyznačením súladu s normami ISO 27017, ISO 27018 apod.) a uviesť mieru súladu bezpečnostnej architektúry služby s dokumentom "Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti"<sup>9</sup>, mieru vzdelávania personálu v oblasti bezpečnosti, popísať oblasť nácvikov riešenia krízových situácií, uviesť podrobnosti o technickom zabezpečení dátových centier, uviesť informácie o riadení prístupov a správe hesiel ako aj mieru ochrany uchovávaných údajov šifrovaním.

4. V ďalšej časti dotazníka záujemca zodpovie špecifické otázky ohľadom zmluvných prevádzkových, technicko-bezpečnostných a platformovo špecifických aspektov, fungovania a prevádzky cloudovej služby.

V hodnotiacom formulári pre cloudové služby sú vyplňané a posudzované oblasti rozdelené do štyroch základných oblastí (ekonomicko – legislatívne údaje, prevádzka služby, bezpečnosť a platformovo špecifické údaje).

---

<sup>8</sup> [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=2327](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2327)

<sup>9</sup> <https://www.csirt.gov.sk/metodika-zabezpecenia-ikt.html>

V oblasti ekonomicko – legislatívnych údajov záujemca vyplňa údaje z nasledovných kategórií: Profil poskytovateľa cloudových služieb, Informácie o fyzickej lokalizácii dátových centier poskytovateľa cloudových služieb, Správa služieb, Detailnejší profil spoločnosti, Referenčné informácie o cloudovej službe, Platné certifikáty, Zmluvné náležitosti, Pravidlá narábania s dátami, Zmluvné požiadavky zabezpečenia a ochrany dát, Zmluva o úrovni poskytovaných služieb (SLA), Podmienky v prípade zastavenia poskytovania zazmluvnených služieb, ceny a nákladové položky za poskytované služby a voliteľné špecifické okruhy otázok.

V oblasti prevádzky hodnotenej služby vyplňa údaje z nasledovných kategórií: Správa a prevádzka dátových centier, Zákaznícka podpora a Správa poskytovaných služieb.

V oblasti bezpečnosti ponúkanej služby záujemca vyplňa údaje z nasledovných kategórií:

- Riadenie bezpečnosti,
- Technická bezpečnosť,
- Technické opatrenia na ochranu osobných údajov.

V oblasti platformovo špecifických údajov ohľadom ponúkanej služby záujemca vyplňa údaje týkajúce sa špecifik jednotlivých platforiem (IaaS, PaaS, SaaS) v nasledovných kategóriách: Systémový manažment, Bezpečnosť, Manažment licencií, Referenčná architektúra, Správa (nasadenie aplikácií do prevádzky), Interoperabilita a Podpora užívateľov.

Ako bolo uvedené v kapitole 1.3.4. vykoná sa hodnotenie podľa nasledujúceho:

- hodnotenie poskytovanej cloudovej služby, cloudová služba **kategórie U2** musí byť posúdená a ohodnotená hodnotiteľom. Hodnotiteľ je akreditovaná osoba, spĺňajúca kritériá uvedené v kapitole 2. Hodnotiteľ.

hodnotenie poskytovanej cloudovej služby, cloudová služba **kategórie U3 a U4** musí byť posúdená a ohodnotená hodnotiteľom. Hodnotiteľom je certifikovaný Audítor kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z.

Hodnotiteľ pre hodnotenie ponúkanej cloudovej služby použije záujemcom vyplnený formulár (príloha 1C\_Formulár pre hodnotenie CS). Pre hodnotenie ponúkanej cloudovej služby kategórie U2, U3, U4 hodnotiteľom, je oproti formuláru pre samohodnotenie v kategórii U1 komplexnejší a detailnejšie pokrýva viac oblastí posudzovanej cloudovej služby.

Pre prácu s formulárom pre hodnotenie cloudovej služby musia byť jednotliví hodnotitelia vyškolení. Školenia pre prácu s formulárom sú neoddeliteľnou súčasťou akreditačného procesu hodnotiteľa.

Hodnotiteľ počas samotného hodnotiaceho procesu musí zachovávať princípy auditu a dodržiavať princípy objektivity, nezáujatosti a nestrannosti.

V rámci hodnotiaceho procesu ponúkanej cloudovej služby hodnotiteľ vykonáva kontrolu odpovedí žiadateľa, overuje pravdivosť alebo platnosť odpovedí, ich súlad s požiadavkami, zároveň overí záujemcom priložený dôkaz, jeho relevantnosť a správnosť.

Hodnotiteľ do formulára zaznamenáva všetky potrebné údaje o splnení respektíve nesplnení požiadaviek, nedostatky alebo nezrovnalosti, prípadne zaznamená svoj komentár k odpovedi, alebo vytvorí požiadavku na doplnenie požadovaných údajov v zrozumiteľnej forme.

Za správnosť a pravdivosť údajov zaznamenaných v dotazníku zodpovedá hodnotiteľ.

V dotazníku hodnotiteľ overuje dokumenty, odkazy, linky na webové sídla s uvádzanými údajmi, ktoré záujemca o poskytovanie cloudovej služby poskytne hodnotiteľovi v listinnej alebo elektronickej podobe, tieto sa stávajú neoddeliteľnou súčasťou hodnotiaceho formulára ako jednotlivé prílohy, pričom túto skutočnosť musí záujemca/hodnotiteľ v hodnotiacom formulári uviesť. V prípade údajov v listinnej podobe, ak sa jedná o údaje overiteľné z verejne prístupných zdrojov postačuje neoverená kópia príslušného dokladu (certifikát, osvedčenie, výpis z obchodného registra), v špecifických prípadoch musí záujemca odovzdať hodnotiteľovi overenú kópiu dokumentu. V prípade údajov v digitálnej forme tieto musia byť uložené na dátovom nosiči (CD alebo DVD disk, USB kľúč apod.), ktorý je čitateľný bežne dostupnými technickými prostriedkami. Dáta a/alebo dátové nosiče sú prílohou hodnotiaceho formulára.

Ak záujemca o poskytovanie cloudovej služby preukáže svoju spôsobilosť alebo kvalifikáciu pre určitú oblasť preverovaných skutočností predložením príslušného certifikátu (napr. certifikácia podľa radu noriem ISO 27000), záujemca do príslušných častí dotazníka uvedie len odkaz na príslušnú certifikáciu a nemusí uvádzať žiadne ďalšie údaje.

Hodnotiteľ následne overí len tie otázky, ktoré nie sú preukázateľné pomocou existujúcich certifikátov (napr. súlad s pravidlami interoperability<sup>10</sup>, vendor lock-in<sup>11</sup> a podobne, ktoré sú súčasťou katalógu vlastností cloudových služieb).

Pri posudzovaní údajov, ktoré poskytol hodnotiteľovi záujemca o poskytovanie cloudovej služby musí hodnotiteľ klásť dôraz na parametre, ktoré sú kvantifikovateľné a merateľné (doba odozvy, reakčná doba služieb podpory, dostupnosť ponúkanej služby).

Za účelom kontroly plnenia požadovaných kritérií hodnotiteľ vykoná kontrolu formulára **1F\_Mapovanie\_Pracovna\_Príloha**, zároveň môže vykonať kontrolu DC prevádzkovateľa cloudovej služby (v prípade ak to bude pokladať za potrebné) a uvedenú kontrolu zaznamená v dokumente **1H\_Protokol o kontrole dátového centra**.

**V prípade, že novo hodnotená cloudová služba prevádzkovaná rovnakým prevádzkovateľom, ako už zapísaná cloudová služba v KsVC ktorá je zapísaná iným poskytovateľom, hodnotiteľ hodnotí len tie časti formulára, ktoré sú špecifické pre nového žiadateľa o zápis práve hodnotenej služby.**

---

<sup>10</sup> <http://www.ecis.eu/2016/06/special-paper-on-cloud-computing-portability-and-interoperability/>

<sup>11</sup> [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=2327](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=2327)

### 3.2.5 Hodnotenie poskytovanej cloudovej služby

Poskytovateľ cloudovej služby musí preukázať, že cloudová služba spĺňa štandardy poskytovania cloud computingu a využívania cloudových služieb podľa štandardov informačných systémov verejnej správy príslušnej kategórie.

Posudzovanie a hodnotenie ponúkanej cloudovej služby závisí od kategórií cloudových služieb.

Pre hodnotenie cloudovej služby kategórie U1 je určené tzv. samohodnotenie. Záujemca vyplní dotazník samohodnotenia (príloha 1B\_Formulár pre samohodnotenie CS), ktorý následne doručí MIRRI. Súčasťou formulára pre samohodnotenie CS je vyhlásenie poskytovateľa cloudových služieb o súlade s príslušnými štandardmi **Chyba! Záložka nie je definovaná.** v rozpise podľa jednotlivých štandardov.

Cloudová služba kategórie U2 musí byť posúdená a ohodnotená hodnotiteľom. Hodnotiteľ pre ohodnotenie ponúkanej cloudovej služby využije formulár vyplnený žiadateľom (príloha 1C\_Formulár pre hodnotenie CS). Hodnotiteľ overí správnosť a úplnosť odpovede a doplní ho o hodnotenie vlastností stanovených kritérií pre kategóriu U2 v spolupráci so žiadateľom. Súčasťou formulára pre hodnotenie CS je vyhlásenie poskytovateľa cloudových služieb o súlade s príslušnými štandardmi<sup>12</sup> v rozpise podľa jednotlivých štandardov.

Pre cloudovú službu kategórie U3 platia rovnaké postupy ako pre kategóriu U2, avšak hodnotenie a posúdenie vykonáva certifikovaný audítor kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Pre cloudovú službu kategórie U4 platia rovnaké postupy ako pre kategóriu U3, avšak cloudové služby tejto kategórie musia byť prevádzkované v privátnej časti vládneho cloudu, hodnotenie a posúdenie vykonáva certifikovaný audítor kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Bližší popis hodnotenia jednotlivých kategórií je popísaný v kapitole **Chyba! Nenašiel sa žiaden zdroj odkazov.** **Chyba! Nenašiel sa žiaden zdroj odkazov..**

Všetky požiadavky pre jednotlivé kategórie sú v prílohách

- **1G\_Popis\_procesov** a
- **1I\_Poziadavky\_na\_zapis\_CS** v tabuľke č.1.

#### 3.2.5.1 Zjednodušený spôsob hodnotenia

V prípade, že poskytovateľ služby akredituje novú službu, ktorá vychádza z už akreditovanej služby, MIRRI môže zredukovať obsah otázok na tie, ktoré slúžia len na dodatočné ohodnotenie.

Ilustračný príklad:

---

<sup>12</sup> § 43 ods. 4 písm. d) vyhlášky Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu č. 78/2020 Z.z. o štandardoch pre informačné technológie verejnej správy v znení vyhlášky Ministerstva investícií, regionálneho rozvoja a informatizácie Slovenskej republiky č. 546/2021 Z. z.

Poskytovateľ firma X má už akreditovanú službu na báze Office365 s vlastným systémom podpory pod svojim vlastným označením. Úrad môže rozhodnúť v prípade firmy Y, že nie je nutné overovať bezpečnostné parametre Office365 znova a požiada firmu Y o vyplnenie len relevantných otázok formulára, ktoré súvisia s nadstavbou ponúkanej služby.

### 3.3 Zápis hodnotenej cloudovej služby do Katalógu cloudových služieb

Po úspešnom priebehu hodnotiaceho a posudzovacieho procesu bude hodnotená a posúdená cloudová služba zapísaná do katalógu cloudových služieb, pričom **platnosť zápisu je 2 roky**. Zoznam úspešne hodnotených a zapísaných cloudových služieb bude zverejnený v príslušnej zložke na webovom sídle MIRRI, a všetky zapísané služby budú zároveň zverejnené v MetaIS.

<https://www.mirri.gov.sk/sekcie/informatizacia/egovernment/vladny-cloud/katalog-cloudovych-sluzieb/>.

Zoznam bude udržiavaný a pravidelne aktualizovaný. V zozname bude uvedený údaj o dobe platnosti zápisu cloudovej služby. Po uplynutí doby platnosti zápisu cloudovej služby stráca táto služba platnosť a ak má poskytovateľ cloudovej služby záujem poskytovať službu aj v ďalšom období, musí ním ponúkaná služba nanovo prejsť celým procesom hodnotenia a posúdenia.

Zápis úspešne ohodnotenej a posúdennej služby do katalógu cloudových služieb vykoná MIRRI v závislosti od príslušnej kategórie cloudovej služby.

Zápis hodnotenej a posúdennej cloudovej služby kategórie U1 vykoná MIRRI na základe **žiadosti** (príloha 1A\_Žiadosť o registráciu CS) a **posúdenia a prípadného overenia údajov z formulára** (príloha 1B\_Formulár pre samohodnotenie CS), ktoré záujemca o zápis cloudovej služby doručí MIRRI.

Ako bolo uvedené v kapitole 3.2.5, MIRRI ako koordinačný a metodický orgán má právo preveriť pravosť a dôveryhodnosť údajov, ktoré záujemca uviedol v dotazníku v priebehu 30 pracovných dní od doručenia vyplneného formulára pre samohodnotenie na MIRRI. V prípade zistenia nedostatkov alebo nezrovnalostí v dotazníku MIRRI vyzve záujemcu na nápravu zistených nedostatkov v termíne do 30 pracovných dní. Ak záujemca do 30 dní vykoná nápravu a nebudú zo strany MIRRI zistené ďalšie nedostatky, MIRRI vydá pokyn na bezodkladný zápis ponúkanej cloudovej služby do KsVC. V prípade zistenia nezhôd alebo závažných nedostatkov a ak záujemca o poskytovanie cloudových služieb tieto nezhody a nedostatky neodstráni do 30 pracovných dní, má MIRRI právo zápis do KsVC odmietnuť a cloudová služba nebude MIRRI zapísaná do Katalógu ponúkaných cloudových služieb.

Zápis hodnotenej a posúdennej cloudovej služby kategórie U2 vykoná MIRRI na základe hodnotenia cloudovej služby hodnotiteľom, ktoré hodnotiteľ cloudovej služby doručí MIRRI. MIRRI bezodkladne zapíše ponúkanú cloudovú službu do KsVC. V prípade zistenia nezhôd alebo nedostatkov má poskytovateľ cloudovej služby na ich odstránenie lehotu 30 pracovných dní.

Zápis hodnotenej a posúdennej cloudovej služby **kategórie U3 a U4** vykoná MIRRI na základe hodnotenia hodnotiteľmi MIRRI bezodkladne zapíše ponúkanú cloudovú službu kategórie U3/U4 do KsVC.

V prípade zistenia nezhôd alebo nedostatkov má poskytovateľ cloudovej služby kategórie U3 na ich odstránenie lehotu 30 pracovných dní. Ak záujemca o poskytovanie cloudovej služby kategórie U3 nevykoná do 30 pracovných dní nápravu, cloudová služba nebude MIRRI zapísaná do Katalógu cloudových služieb.

### 3.4 Monitoring a kontrola kvality poskytovania CS

Základnými požiadavkami pre stabilné, spoľahlivé a bezpečné používanie cloudovej služby je dodržiavanie deklarovaných parametrov prevádzkovej cloudovej služby. Parametre cloudovej služby sú uvedené v zmluve o úrovni poskytovaných služieb (Service Level Agreement, SLA), ktorá je neoddeliteľnou súčasťou zmluvy o poskytovaní cloudových služieb a je zároveň jedným z kľúčových faktorov procesu overovania a samotnej akreditácie poskytovanej cloudovej služby. Miera definovaných parametrov v zmluve SLA určuje mieru kvality a úroveň prevádzkovej cloudovej služby.

Zároveň parametre prevádzkovej cloudovej služby určujú kategóriu cloudovej služby (U1, U2, U3, U4). Pre každú kategóriu sú požiadavky na parametre v zmluve SLA odlišné (čím vyššia kategória, tým náročnejšie parametre a podmienky) a zároveň úroveň parametrov, definovaná v zmluve SLA má priamy vplyv na cenu poskytovanej služby. Za dodržiavanie parametrov cloudovej služby, definovaných v zmluve SLA je zodpovedný poskytovateľ cloudovej služby.

Pre posúdenie, či cloudová služba, uvedená v Katalógu poskytovaných cloudových služieb spĺňa parametre deklarované poskytovateľom, je nutné tieto parametre kontrolovať a monitorovať. Základnou vlastnosťou deklarovaných parametrov, definovaných v zmluve SLA, potrebnou pre ich kontrolu je ich merateľnosť.

MIRRI monitoruje a kontroluje kvalitu poskytovaných cloudových služieb zaradených do katalógu, minimálne formou overovania dostupnosti ponúkaných služieb a kontrolou merateľných parametrov SLA.

V prípade zistenia nedostatkov alebo nezhôd podľa miery závažnosti, MIRRI vyzve poskytovateľa cloudovej služby na zdôvodnenie a nápravu v lehote **30** kalendárnych dní. Zároveň MIRRI s touto skutočnosťou oboznámi používateľov, pričom ich upozorní na skutočnosť, že ak po uplynutí termínu na nápravu zistené nedostatky a nezhody nebudú odstránené, poskytovanie cloudovej služby bude zastavené a služba bude vymazaná z Katalógu cloudových služieb.

#### 3.4.1 Roly a povinnosti MIRRI

Hlavným riadiacim a kontrolným orgánom, spravujúcim KsVC je MIRRI.

MIRRI zároveň zodpovedá za kontrolu úrovne a kvality poskytovaných cloudových služieb a je hlavným partnerom pre komunikáciu s poskytovateľmi cloudových služieb a hodnotiteľmi. V zmysle zákona č. 95/2019 Z.z. § 24a odstavce 3 a 4.

MIRRI disponuje právomocou rozhodovať o zapísaní cloudovej služby do KsVC, o suspendovaní alebo vyčiarknutí cloudovej služby z KsVC na základe informácií alebo podnetov od relevantných

subjektov. Relevantnými subjektmi sú poverení pracovníci MIRRI, hodnotitelia ale aj používatelia – OR, ktorí majú právo informovať MIRRI o nesúlade alebo nedodržiavaní parametrov SLA poskytovateľom cloudovej služby. MIRRI riadi tiež proces výberu prípadne schvaľovania hodnotiteľov, ktorého popis je v dokumente „1E\_Popis hodnotiteľa CS“.

Medzi povinnosti MIRRI patrí overovanie a kontrola údajov a informácií, ktoré uvedie záujemca o poskytovanie cloudovej služby v procese akreditácie ponúkanej cloudovej služby kategórie U1 vo formulári pre samohodnotenie (príloha 1B\_Formulár pre samohodnotenie CS). Vo fáze overenia súladu MIRRI vykonáva administratívnu kontrolu a overenie uvedených údajov, nakoľko záujemca o akreditáciu ponúkanej cloudovej služby v tejto fáze ešte nemusí mať ponúkanú službu dostupnú v produktívnej prevádzke a kontrola merateľných parametrov, definovaných v zmluve SLA by nemusela byť realizovateľná.

Počas produkčnej prevádzky cloudovej služby uvedenej v KsVC, zamestnanci MIRRI vykonávajú kontrolu merateľných parametrov cloudovej služby, ktoré eviduje v MetaIS poskytovateľ (doba odozvy, dostupnosť služby, reakčná doba centra klientskej podpory Help Desk a pod.).

Používatelia cloudovej služby zaznamenávajú spokojnosť s prevádzkou poskytovanej cloudovej služby do MetaIS.

### 3.4.2 Proces zistenia nesúladu služby

Ak počas procesu monitoringu a kontroly poskytovanej cloudovej služby zapísanej v KsVC MIRRI identifikuje nesúlad alebo nedodržiavanie parametrov poskytovanej cloudovej služby definovaných v zmluve SLA, je MIRRI povinné v zmysle tohoto metodického usmernenia a zákona<sup>13</sup> začať nápravný proces. Podnetom pre začatie nápravného procesu je záznam z kontroly poskytovanej cloudovej služby alebo podnet (sťažnosť) zo strany používateľa cloudovej služby – OR.

MIRRI bezprostredne po prijatí podnetu alebo identifikácii nezhody oboznámi poskytovateľa cloudovej služby zapísanej v KsVC s identifikovanými nedostatkami alebo nesúladom parametrov poskytovanej cloudovej služby s parametrami, uvedenými v zmluve SLA. Zároveň vyzve poskytovateľa cloudovej služby na okamžité vykonanie nápravy a uvedenie parametrov poskytovanej cloudovej služby do súladu s parametrami definovanými v zmluve SLA.

O zistených nedostatkoch a nesúlade parametrov poskytovanej cloudovej služby s parametrami definovanými v zmluve SLA, MIRRI informuje aj používateľov poskytovanej cloudovej služby – OR, pričom ich zároveň oboznámi s lehotou, ktorú má poskytovateľ cloudovej služby na zjednanie nápravy a uvedenie parametrov poskytovanej služby do súladu so zmluvou SLA.

Pri zistení výrazného nesúladu služby, MIRRI informuje relevantné tretie strany (Sekciu kybernetickej bezpečnosti, CSIRT, ...)

Poskytovateľ cloudovej služby má na realizáciu nápravy a uvedenie do súladu so zmluvou SLA najviac 30 dní. Ak do tejto lehoty nebude zjednaná náprava a parametre služby nebudú uvedené do súladu s parametrami zmluvy SLA, poskytovaná cloudová služba bude pozastavená.

---

<sup>13</sup> Zákon 95/2019 Z.z. § 24a Vládný cloud, odsek 4.

O tejto skutočnosti musí MIRRI informovať uvedením poskytovanej cloudovej služby v Katalógu cloudových služieb na svojom webovom sídle do pozastaveného stavu. S touto skutočnosťou musia byť zároveň bezprostredne oboznámení používatelia cloudovej služby – OR, pričom ich MIRRI vyzve na prijatie príslušných opatrení (napr. obstaranie cloudovej služby od iného poskytovateľa, stiahnutie spracovávaných údajov z úložiska končiaceho poskytovateľa, nájdenie alternatívneho riešenia).

V prípade, ak ani počas ďalších **30** dní nebude zjednaná náprava a parametre poskytovanej cloudovej služby nebudú uvedené do súladu s parametrami zmluvy SLA, poskytovaná cloudová služba bude z KsVC vyčiarknutá. MIRRI vyzve poskytovateľa cloudovej služby na bezodkladné ukončenie poskytovania cloudovej služby používateľom a vyčiarkne službu z KVCS a o vymazaní informuje všetkých používateľov.

### 3.5 Ukončenie poskytovania služby

V prípade ukončenia poskytovania cloudovej služby (z dôvodu zániku/neplatnosti akreditácie, pri bankrote poskytovateľa cloudovej služby a pod.) má MIRRI povinnosť informovať používateľov cloudovej služby o presnom termíne ukončenia poskytovania cloudovej služby.

Ak je dátum ukončenia poskytovania cloudovej služby známy (ak napr. poskytovateľ nechce pokračovať v prevádzke cloudovej služby), MIRRI je povinný s touto skutočnosťou oboznámiť používateľov (OR) včas a s dostatočným predstihom.

#### 3.5.1 Vyradenie zapísanej cloudovej služby z Katalógu cloudových služieb

Doba platnosti akreditácie cloudovej služby, zapísanej v KsVC je 2 roky od dátumu zápisu. Po uplynutí platnosti služby v prípade ak má poskytovateľ služby záujem o jej ďalšie poskytovanie musí poskytovateľ nanovo požiadať o zápis služby do katalógu služieb **Dva mesiace pred uplynutím platnosti** akreditácie cloudovej služby MIRRI ako riadiaci a kontrolný orgán **upovedomí poskytovateľa cloudovej služby** o blížiacom sa konci platnosti akreditácie cloudovej služby. Poskytovateľ má na opätovnú akreditáciu cloudovej služby 2 mesiace.

Poskytovateľ cloudovej služby musí MIRRI oznámiť, či mieni pokračovať v poskytovaní cloudovej služby. Na základe tejto informácie MIRRI oboznámi príslušných používateľov predmetnej cloudovej služby (OR) o blížiacom sa konci platnosti akreditácie cloudovej služby. Zároveň bude dotknuté OR informovať o zámere poskytovateľa pokračovať/nepokračovať v poskytovaní cloudovej služby. V prípade, ak poskytovateľ nemá záujem pokračovať v poskytovaní cloudovej služby, tak musí dotknutým OR zabezpečiť dostatočný časový priestor na zabezpečenie iného riešenia minimálne však 6 mesiacov.

V prípade záujmu pokračovať v poskytovaní cloudovej služby musí poskytovateľ zahájiť proces akreditácie poskytovanej cloudovej služby. Novú akreditáciu cloudovej služby je povinný predložiť najneskôr k dátumu ukončenia platnosti doposiaľ platnej **akreditácie**.

Ak k dátumu ukončenia platnosti akreditácie poskytovanej cloudovej služby nebude akreditačný proces cloudovej služby úspešne ukončený, v KsVC na webovom sídle pri predmetnej cloudovej službe MIRRI zverejní poznámku „**V akreditačnom procese**“.

Ak do 30 dní od uplynutia platnosti akreditácie poskytovateľ prevádzkovej cloudovej služby nepredloží MIRRI novú žiadosť o zápis poskytovanej služby do KsVC, predmetná cloudová služba prejde do suspendovaného stavu a poskytovateľ musí oznámiť túto skutočnosť svojim klientom/OR.

Ak následne do **60** dní poskytovateľ nepredloží novú žiadosť o zápis poskytovanej služby do KsVC, táto služba bude z KsVC vymazaná. MIRRI zároveň upovedomí ako používateľov predmetnej cloudovej služby (OR), tak aj poskytovateľa predmetnej cloudovej služby o vymazaní (vyrazení) tejto cloudovej služby z KsVC.

V tomto prípade musí poskytovateľ zabezpečiť dotknutým OR dostatočný časový priestor na obstaranie iného riešenia minimálne však 6 mesiacov.

### 3.5.2 Ukončenie poskytovania služby na žiadosť poskytovateľa

V prípade ukončenia poskytovania cloudovej služby (na základe žiadosti poskytovateľa cloudovej služby), poskytovateľ cloudovej služby je povinný zabezpečiť poskytovanie služby na dostatočne dlhú dobu, aby používatelia OR mali dostatočný čas na prijatie príslušných organizačných a technických opatrení (napr. obstaranie potrebnej služby od iného poskytovateľa).

MIRRI je povinný s touto skutočnosťou oboznámiť používateľov (OR) včas a s dostatočným predstihom.

## 4 Povinnosti OR pri využívaní služby zapísanej v KsVC

Cloudové služby uvedené v KsVC sú predovšetkým určené pre používanie orgánmi riadenia (OR). Proces obstarávania cloudových služieb a ich prevádzkovanie nie je predmetom tohto metodického usmernenia, ale používateľom pri ich využívaní vznikajú určité povinnosti s cieľom zamedzenia prípadných prevádzkových problémov pri ich využívaní.

### 4.1 Registrácia používania služby

Používateľ cloudovej služby (OR), zapísanej v Katalógu služieb vládneho cloudu má povinnosť zaevidovať používanie cloudovej služby k ISVS do MetaIS.

Cieľom registrácie je informačná povinnosť MIRRI, ktorý v prípade vzniku neštandardnej situácie poskytovateľa cloudovej služby bezprostredne oboznámi všetkých dotknutých používateľov s informáciami o vzniknutej situácii (prevádzkové a technické problémy prevádzkovateľa cloudovej služby, nesúlad a nedodržanie zaručených parametrov SLA, nedodržanie podmienok služby podpory apod.).

MIRRI môže OR informovať o možných scenároch ďalšieho vývoja (možnosť suspendovania poskytovanej služby na určité obdobie, zánik poskytovanej cloudovej služby od dátumu ukončenia platnosti jej akreditácie) a zároveň môže OR vyzvať na prijatie príslušných opatrení (napr. obstaranie cloudovej služby od iného poskytovateľa, stiahnutie spracovávaných údajov z úložiska končiaceho poskytovateľa, alternatívne riešenia).

Registrácia používaných cloudových služieb je zo strany OR povinná.

## 5 Prílohy

Všetky dokumenty a dotazníky sú dostupné na webovom sídle MIRRI: <https://www.mirri.gov.sk/sekcie/certifikacia-a-zapis-sluzieb-vladneho-cloudu/>, a sú k dispozícii pre každého záujemcu.

1A\_Žiadosť o registráciu CS

1C\_Formulár pre hodnotenie CS

1D\_Katalóg vlastností CS

1E\_Popis hodnotiteľa CS  
1F\_Mapovanie\_Pracovná\_Príloha  
1G\_Popis\_procesov  
1H\_Protokol o kontrole dátového centra  
1I\_Požiadavky\_na\_zápis\_CS  
1J\_Hodnotenie hodnotiteľom – kontrolný formulár hodnotiteľa  
1K\_Úrovne\_cloudových\_služieb\_na\_zápis\_CS  
1L\_Štandardy\_Súlاد