**Záznam z prípravných trhových konzultácií**

podľa § 25 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“)

**1. Identifikácia verejného obstarávateľa:**

**Názov:** Ministerstvo investícií, regionálneho rozvoja a informatizácie SR (ďalej len „MIRRI SR“)

**Organizačný útvar:** Odbor verejného obstarávania,

**Sídlo:** Pribinova 25, 811 09 Bratislava

**IČO:** 50349287

**DIČ:** 2120287004

**Kontaktná osoba:**, Mgr. Martin Nociar, Kristián Hodossy; Anton Svetlošák

**Tel.:** +421 2 2092 8102; +421 2 2092 8195

**E-mail:** martin.nociar@mirri.gov.sk; kristian.hodossy@mirri.gov.sk, anton.svetlosak @mirri.gov.sk

**Adresa hlavnej stránky verejného obstarávateľa:** www.mirri.gov.sk

**2. Identifikácia účastníka prípravných trhových konzultácií:**

**Poskytovateľ cloudových služieb:** účastník PTK 2

Pre účely záznamu z prípravných trhových konzultácií (ďalej len „PTK“), ktorý je publikovaný na webovom sídle verejného obstarávateľa, je identifikácia účastníkov trhu anonymizovaná. Verejný obstarávateľ eviduje zoznam účastníkov PTK ako súčasť kompletnej dokumentácie k postupu zadávania zákazky.

**3. Názov zákazky:**

“ *Obstaranie cloudových služieb, a príbuzných podporných služieb.* "

**4. Spôsob vykonania a priebeh prípravných trhových konzultácií:**

Prípravné trhové konzultácie boli iniciované e-mailovým oslovením štyroch potenciálnych poskytovateľov predmetu zákazky za účelom možného doplnenia opisu predmetu zákazky. Prílohou zaslaného e-mailu zo dňa 2.6.2022 bolo Oznámenie o začatí prípravných trhových konzultácií, návrh zmluvy a Opis predmetu zákazky (OPZ). Formulár na prihlásenie sa do PTK. Verejnému obstarávateľovi boli doručené odpovede od poskytovateľa cloudovej služby.

**5. Odpovede na otázky sú uvedené v prílohe č.2:**

**6. Záznam zo dňa: 21.6.2023**

Boli predstavení účastníci p. Svetlošákom za stranu MIRRI – za technické veci p.Gelien a p. Tomášek, za právne veci p. Hodossy a taktiež technickí a právni špecialisti za stranu poskytovateľa.

**Prvá otázka** zo strany MIRRI bola, či požiadavky RFI sú dosiahnuteľné a či poskytovateľ vidí dajaké prekážky na dodanie takéhoto riešenia.

**Odpoveď:**

Poskytovateľ pochopil naše zadanie a potreby, a sú si vedomí, ktoré veci v riešení nepokryjú. Dedikovaný region vie pokryť naše potreby. Jednou z vecí ktorú treba prediskutovať je IO operations. Vedia, že budú dodávať on-prem riešenie - dedikovaný region a IO operations majú na roadmape. Sovereign cloud bude k dispozícii už čoskoro a viacej vecí musí byť zmanažovaných. Je to pre nich výzva z časového hľadiska.

Ak IO operations je požadované z našej strany, všetky dáta sú kryptované a kľúče sú uložené v dedikovanom regione.

 Ak si zákazník prinesie vlastné kľúče, je to veľký rozdiel. Majú spoluprácu s firmou dodávajúcou HSM, ktorý poskytuje HSM modul. Tento HSM modul môže byť on-premise alebo umiestnený aj mimo cloudu. Môže ho mať zákazník u seba a kľúče sa neprenášajú-neopustia HSM. Tým sú izolované. Poskytovateľ tým pádom nemá prístup ku kľúčom a nemá vôbec prístup k dátam. Z pohľadu Cloud act, všetky dáta sú kryptované a keď poskytovateľ dostane príkaz poskytnúť dáta tretej strane, tie sú kryptované kľúčmi zákazníka a dáta sú nedostupné pre kohokoľvek.

Pre MIRRI je toto riešenie preferované a výhodné.

**Otázka**:

Keď je HSM mimo on-premise cloudu, ako je to z SLA podporou? Poskytuje to poskytovateľ ako jeden balík?

Odpoveď: Ak je HSM mimo public cloud ,alebo Sovereign cloud, alebo on-premise cloud, je to mimo IO operations modelu. Vedia poskytnúť v súčasnosti len global operations. IO personal nedostaneme ak budeme mať dedikovaný region.

Poskytovateľ pracuje na zriadení právnej EU entity na manažovanie všetkých assets, ktorí by poskytoval suverenitu založenú na legislatíve.

**Otázka**:

Spadá dedikovaný region pod Cloud act tak isto ako OCI?

**Odpoveď**:

Je to otázka času, technické záležitosti musia byť vyčlenené.

Vytvorenie novej legislatívnej entity je to výzva do budúcna. Poskytovateľ na tom pracuje ale zaberie to veľa času.

Road mapa a time line ešte nie je známa. Musí byť vyjasnených a zodpovedaných veľa otázok.

Potrebujú požiadavky z legislatívnej oblasti. Teraz nemôžu zabezpečit suverenitu z právneho hladiska.

Poskytovateľ tvrdí, že cloud act je len pre public cloud, nie pre privátny.

Poskytovateľ musí vedieť, či Cloud act sa týka aj privátnych cloudov a oznámiť nám túto skutočnosť.

**Otázka**:

Sovereign cloud nie je podporovaný v dedicated region ?

**Odpoveď**:

Pracujú na tom a je to otázka času, kedy bude Sovereign cloud aj pre dedicated region. Musia vytvoriť právne entity v každej krajine, kde sa nachádza zariadenie od poskytovateľa. Je to otázka aj daňových predpisov a zákonov. Hľadajú riešenie, ako to dosiahnuť. Teraz ešte nemajä jasno, čo a ako to dosiahnuť. Ešte nevedia time-line ani roadmapu.

Je to pre MIRRI problem – lebo musíme schváliť kontrakt, ktorý bol pripomienkovaný. Robíme tieto rozhovory s viacerými poskytovateľmi. Cieľ je zmluva, ktorá je vendor neutrálna. Sovereign entity je problém pre poskytovateľov ale aj pre MIRRI z hľadiska security.

Naša požiadavka bola, že prístup do dedikovaného regionu má mať len IO operations a nie Global operations.

**Otázka**:

Sovereign cloud nie je možný pre dedicatet region ?

**Odpoveď**:

Áno.

**Otázka**:

Poskytovateľa by zaujímalo, aké sú naše právne predpisy čo sa týka Sovereign cloudu, prečo nemôže zariadenia vlastniť lokálny zástupca v našej krajine a IO by mohlo byť globálne.

**Odpoveď**:

Naše predpisy boli zapracované do návrhu zmluvy, ktoré boli poslané poskytovateľovi.

V riešení chceme byť nezávislý od iných právnych noriem iných štátov ako EU.

**Otázka**:

Poskytovateľ má SLA pre public cloud. Môžeme ho dostať ?

 Má poskytovateľ SLA pre dedikovaný region ?

**Odpoveď**:

Nie pre dedikovaný region, SLA je rovnaká ako pre public cloud. Pošlú link na public dokument.

Dedicated reagion je postavený na rovnakej technológii ako public cloud.

**Otázka**:

Poskytovateľ namietal, že v zmluve je vec, ktorá nemôže byť akceptovaná z jeho strany. Máme to chápať, že poskytovateľ to nikdy nebude akceptovať ?

**Odpoveď**: Bolo to už diskutované s tým, že poskytovateľ má svoje terms a conditions a veci v zmluve nie sú relevantné pre privátny region. Bolo by to ťažké akceptovať to. Poskytovateľ predpokladá ďaľšie diskusie na túto tému. Poskytovateľ musí mať tú vec v zmluve schválenú z vyšších štruktúr ale nevie kedy to bude.

**Otázka**:

Môže poskytovateľ jednať so zástupcami MIRRI priamo alebo prostredníctvom mailovej komunikácie ?

**Odpoveď**:

Nie, nemôžu už komunikovať. Len keď budú oslovení MIRRI a bude ďaľšie kolo PTK. Veci týkajúce sa VO sa konzultujú cez EVO.

Ak potrebujeme ešte nejaké podnety, môžu ich zaslať mailom cez p. Nociara.

**Otázka**:

Poskytovateľ by chcel presne vedieť legislatívne požiadavky, kde je uvedené, že dáta nesmú opustiť územie EU.

**Odpoveď**:

Musíme to konzultovať s právnym oddelením a zašleme.

**Otázka**:

Je potrebné mať zriadenú EU entitu pred podpisom zmluvy alebo stačí ju mať po implementácii riešenia ?

**Odpoveď**:

Poskytovateľ nevie zodpovedať túto otázku. Musia najprv spraviť roadmapu.

Nevedia zaručiť, že sa bude dať prejsť z Global na Sovereign model. Najprv si musia vyriešiť technické veci.

**Otázka**:

Ako dlho bude trvať interné schvaľovanie pre naše legislatívne predpisy ?

**Odpoveď**:

Nie je to časovo náročné, za jeden-dva týždne. Je to unlimited liability . Otázka je či to bude vôbec schválené.

Obchodné podmienky a support musia byť schválené ale nebude to hneď teraz. Poskytovateľ pripravil legislatívu, ktorá hovorí, že dáta neopustia EU – poskytnú odpoveď.

EU operations team – nevedia sa vyjadriť, pokiaľ nie je legislatíva. Pracujú na road mape.

Unlimited liability – toto môže byť show stoper. MIRRI potrebuje nastaviť time line pre procurement.

Poskytovateľ potrebuje vedieť presne naše legislatívne podmienky a od toho sa odvíja hľadanie riešenia a schvaľovanie. Ak sú to len technikálie, musí do toho byť zapojený aj technický tím.

Poskytovateľ potrebuje vedieť timeline ktorý je závislý na US cloude.

**Otázka**:

Kde sa nachádzajú technické veci alebo cloud opatrenia, ktoré sú potrebné pre budúci kontrakt?

**Odpoveď**:

Sú verejne dostupné. V Nemecku sa tomu venuje kolega, ktorý má tieto veci na starosti.

V Nemecku nemali veľa diskusií ohľadne Cloud actu a nie je to ich top priorita. Majú vytvorený team podobný ako má US cloud a používajú rovnakú entitu. Veľa diskusií mali na tému technických vecí a security BSI, procesy ktoré musia byť implementované, odpoveď na icidenty atď.

Prebiehajú technické opatrenia – cloud act je veľká téma.

V Nemecku robí spoločnosť BSI zastúpenie namiesto poskytovateľa z USA, ktorá budovala aj EU cloud. Mali to jednoduchšie, lebo tu je koincidencia s EU cloudom a mohli využiť rovnakú právnu entitu ako má EU. BSI vytvorila a vlastní vládny cloud. Taktiež v Španielsku bolo vybudované datacentrum pre vládny cloud. Je to vždy aj otázka daňových zákonov v danej krajine.

**Otázka**:

Je možné využiť spoločnosť, ktorá spravuje privátne vládne cloudy v Nemecku a Španielsku na manažovanie on-premise cloudu na Slovensku ?

**Odpoveď**:

Nemôžeme využiť BSI aj pre Slovenský eSKa cloud – rôzna legislatíva a daňové zákony. Neexistuje spoločnosť, ktorej pôsobnosť by bola pre celú EU.

Government cloud v Nemecku bude manažovaný personálom z EU, čo môže byť aj náš prípad pre eSKa cloud.

HW musí byť dodaný SK spoločnosťou, tá musí vlastniť HW kvôli internej legislatíve a daniam.

**Otázka**:

Ako poskytovateľ cloudu robí separáciu tenantov?

**Odpoveď**:

Čo sa týka IO operations poskytovateľ vytvoril lokálne tímy v krajinách kde má personál. Tu sú viaceré aspekty. Jednak personál IO operations a vlastník hardware v tej ktorej krajine. Nemajú personál IO operations naprieč EU. Museli by vytvoriť spoločnosť na Slovensku, ktorá by vlastnila HW a podliehala Slovenským zákonom a daniam.

**Otázka**:

Ako je riešené multitenancy?

**Odpoveď**:

Multitenancy v public cloude je zabezpečené na úrovni sieťovej vrstvy. Privátny region bude izolovaný taktiež na sieťovej úrovni.

**Otázka**:

Ako môže byť implementované HSM v on-premise dedicated region ?

**Odpoveď**:

HSM môže byť umiestnené aj v dedicated regione konzumujúci kredity alebo mimo region. Bude to ohlásené. Záleží kedy to firma dodávajúca HSM ohlási a poskytovateľ ho zabuduje aj do dedicated regionu. Vlastný HSM modul môže byť implementovaný v dedicated region.

Na nákup HSM môžu byť použité kredity. Externé HSM je on top a môže byť integrované do dedikovaného regionu.

MIRRI eviduje požiadavky iných OVM, ktoré by chceli využívať HSM, len nevieme o ktoré konkrétne majú záujem. Potrebovali by sme list podporovaných HSM modulov od poskytovateľa, ktoré môžu byť integrované v dedicated region. Nemá zmysel HSM umiestňovať mimo regionu kvôli latencii.

**Otázka**:

Môžu poskytnúť architektonickú dokumentáciu ako majú navrhnutý on-premise cloud v Nemecku?

**Odpoveď**:

Multitenancy v dedicated region je rovnaké ako v public cloude. Vládny cloud je zložený z viacerých regionov. Multitenancy je implementované v Nemeckom vládnom cloude. Jediný rozdiel oproti vládnemu cloudu je že dedicovaný region je single tenant. Ale multitenancy v dedicated region je vytvorená z child-tenancy.

Platí vzťah jeden region = jeden tenant.

Ak je v jednom regione jeden tenant, dá sa nastaviť izolácia. Dá sa nastaviť parent-child model.

Dedicated region – poskytuje plnú funkcionalitu ako v public cloude, confidential computing, security, atd. Je rozdiel vo fakturovaní služieb v parent-child tenancy.

Potrebné kontaktovať právne oddelenie a doriešiť umiestnenie dát, HSM moduly atď.