MESTO KOŠICE

Magistrát mesta Košice
Trieda SNP 48/A, 040 11 Košice

Spis č.: MK/A/2025/19238

Vysvetlenie súťažných podkladov č. 7

Verejný obstarávateľ: Mesto Košice, Trieda SNP 48/A, 040 01 Košice

Názov zákazky: „KONTO KOŠIČANA“

Na základe žiadosti o vysvetlenie súťažných podkladov, ktoré nám bolo doručené v systéme JOSEPHINE dňa 06.08.2025 poskytujeme nasledovnú odpoveď:

1. Otázka:
V dokumente „vysvetlenie súťažných podkladov č.2“ odpovedá verejný obstarávateľ na prvú otázku ohľadom poskytnutia ERD. Otázka sa týka existencie ERD alebo obdobného prehľadu dátovej štruktúry – nie na to, aký vývojový prístup sa má použiť. Odpoveď vytvára zmätok, či vôbec existuje nejaký ucelený pohľad na dáta, čo vnímame ako problém. Ak existuje OpenAPI, mala by byť vysvetlená ako "náhrada ERD" a taktiež uvedené, ako a kde sú entity previazané. Žiadame verejného obstarávateľa potvrdiť existenciu takého dátového modelu pre systém Konto Košičana vo forme ERD alebo databázového diagramu, ako aj prípadne vygenerovaného z OpenAPI.

- Ak áno, prosíme o jeho konkrétne poskytnutie alebo lokalizáciu (napr. príloha, odkaz, súbor).
- Ak nie, prosíme jasne uviesť dôvod jeho absencie a ako je zabezpečený súlad a konzistentnosť dát medzi modulmi (najmä profil, platby, notifikácie a výmery).

Odpoveď:
Verejný obstarávateľ nedisponuje samostatným dokumentom vo forme ERD ani explicitným databázovým diagramom. Na základe súťažných podkladov, vrátane zdrojových kódov, DNR a sprístupnenej OpenAPI špecifikácie, však verejný obstarávateľ považuje dostupné informácie za dostatočné na pochopenie architektúry systému, vzťahov medzi entitami a ich použitia v jednotlivých moduloch.

OpenAPI špecifikácia plnohodnotne plní funkciu dátového modelu z pohľadu návrhu rozhraní, dátových kontraktov a väzieb medzi jednotlivými časťami systému. Z nej je možné vyvodiť väzby medzi entitami, ako aj logiku ich spracovania v rámci integračných rozhraní. Túto špecifikáciu preto vnímame ako relevantnú náhradu formálneho ERD.

Vzhľadom na vyššie uvedené zastávame názor, že absencia samostatného ERD nemá vplyv na schopnosť spracovania ponuky, nacenenie ani samotnú realizáciu predmetu zákazky, nakoľko konzistentnosť a integrita dát je zabezpečená prostredníctvom jednotného dátového modelu obsiahnutého v rámci API rozhraní.

Verejný obstarávateľ mesto Košice po uzatvorení zmluvy zabezpečí Dodávateľovi plnú súčinnosť a zabezpečí plný prístup k servisom a databázam systému Konta Košičana.

2. Otázka:
V dokumente „vysvetlenie súťažných podkladov č.2“ odpovedá verejný obstarávateľ na tretiu otázku ohľadom integrácie na ďalšie informačné systémy. Odpoveď uvádza iba dva systémy (Norris a Helios) a systémy tretej strany bez vysvetlenia ich rozsahu, funkcie či modulov. Chýbajú ďalšie relevantné informácie, ktoré moduly sú producentmi a ktoré konzumentmi a aké IS sa majú integrovať. Vedú systémy NORIS a HELIOS aj evidenciu parkovacích kariet, kariet ZŤP? Bude Konto Košičana predpisovať integračné rozhrania na akýkoľvek systém?

Žiadame uviesť konkrétny zoznam všetkých informačných systémov, na ktoré má byť Konto Košičana integrované alebo s ktorými má výhľadovo komunikovať.
Pre každý uvedený systém uveďte:

- Názov systému a jeho funkčný účel (napr. evidencia obyvateľov, správa daní, parkovanie, ekonomika atď.).
- Prevádzkovateľ/majiteľ systému (napr. mesto, DPMK, Správa parkovísk...).
- Typ rozhrania dostupného pre integráciu (napr. REST API, SOAP, priame DB pripojenie, exporty).

V prípade plánovaných alebo otvorených integrácií s tretími stranami (napr. DPMK, Parkdots, Sčítanie obyvateľov, Slovensko.sk), prosíme identifikovať:

- Konkrétnu tretiu stranu
- Typ integrácie
- Zodpovednosť za technickú a prevádzkovú realizáciu tejto integrácie (mesto, dodávateľ, tretia strana).

Odpoveď:
V zmysle súťažných podkladov a na základe aktuálne známych požiadaviek sa v rámci dodávky systému Konto Košičana počíta s integráciou na nasledovné informačné systémy:

1. Norris

- **Funkčný účel**: Agendový systém mesta Košice, evidencia obyvateľov, správa podnetov, evidencia a spracovanie údajov občanov.
- **Prevádzkovateľ**: Mesto Košice
- **Typ rozhrania**: REST API (špecifikácia bude poskytnutá po podpise zmluvy)
- **Moduly relevantné pre Konto Košičana**:
  - KKProfile – rozšírenie údajov o občanovi a ich správa (Norris je zdroj aj cieľ)
  - KKIniciative – spracovanie podnetov občana a napojenie na workflow (Norris je zdroj aj cieľ)
  - KKNotification – odosielanie správ a notifikácií na základe udalostí (Norris je zdroj)
  - KKCard – správa kariet evidovaných v rámci kompetencie mesta (Norris je zdroj)
- **Poznámka**: Slúži ako zdroj alebo cieľ údajov súvisiacich s občanom a správou podnetov.
- **Zodpovednosť za integráciu**: Mesto Košice zabezpečí potrebnú súčinnosť a prístup k rozhraniam, dátam. Technickú realizáciu pre časť Konto Košičana zabezpečí Dodávateľ.

2. Helios

- **Funkčný účel**: Ekonomický a účtovný systém (napr. správa daní, poplatkov, výmerov a fakturácia)
- **Prevádzkovateľ**: Mesto Košice
- **Typ rozhrania**: REST API (špecifikácia bude poskytnutá po podpise zmluvy)
- **Moduly relevantné pre Konto Košičana**:
  - KKProfile – rozšírenie údajov o občanovi (Helios je zdroj)
- **Poznámka**: Slúži ako zdroj údajov súvisiacich s ekonomickými agendami občana.
- **Zodpovednosť za integráciu**: Mesto Košice zabezpečí potrebnú súčinnosť a prístup k rozhraniam, dátam. Technickú realizáciu pre časť Konto Košičana zabezpečí Dodávateľ.

Systémy tretích strán (min. jedna otvorená integrácia)

Parkdots

- **Funkčný účel:** Evidencia parkovacích kariet
- **Moduly relevantné pre Konto Košičana**:
  - KKCard – správa kariet evidovaných v rámci 3 strany (v kompetencii mesta, Parkdots je zdroj)
- **Typ rozhrania**: REST API (alebo podľa dodávateľa služby)

- **Zodpovednosť**: Mesto Košice zabezpečí potrebnú súčinnosť a prístup k rozhraniam. Technickú realizáciu pre časť Konto Košičana zabezpečí Dodávateľ.

3. Otázka:
Aká konkrétna technologická platforma tvorí ESB infraštruktúrnu vrstvu mesta Košice? Môžete popísať, aká je architektúra a logika integrácie medzi 12 uvedenými modulmi systému Konto Košičana? Prebieha integrácia všetkých modulov cez ESB, alebo sú niektoré moduly integrované priamo medzi sebou (point-to-point)? Za aké všetky činnosti pri ESB má byť dodávateľ zodpovedný?

Odpoveď:
V súvislosti s otázkou týkajúcou sa technologickej platformy, architektúry a integrácie modulov systému Konto Košičana, si dovoľujeme poskytnúť nasledovné vysvetlenie:

Technologická platforma ESB infraštruktúry mesta Košice

ESB infraštruktúrna vrstva nie je postavená na špecializovanej middleware alebo integračnej platforme (napr. WSO2, Mulesoft, Apache ServiceMix). Ide o vlastnú integračnú vrstvu postavenú na infraštruktúre poskytovanej v rámci Orange Cloudu, ktorej komponenty pozostávajú najmä z Firewallov, Load balancerov, Reverse proxy a Virtuálnych serverov (VMs).

Integrácia medzi systémami (vrátane jednotlivých modulov Konto Košičana) je riešená prostredníctvom REST API rozhraní, ktoré komunikujú cez zabezpečené kanály (HTTPS) v rámci vyššie uvedenej infraštruktúry.

Architektúra a logika integrácie medzi 5 (v súčasnosti existuje 5 modulov, nie 12) modulmi systému Konto Košičana

Modulárna architektúra systému Konto Košičana umožňuje oddelený vývoj, nasadenie a škálovanie jednotlivých modulov. Každý modul má definované vlastné rozhranie (API), ktorým komunikuje s ostatnými modulmi alebo so systémami tretích strán.

- Hlavná integračná logika medzi modulmi je zabezpečená cez zverejnené a zdokumentované REST API.
- Niektoré moduly môžu komunikovať priamo medzi sebou (point-to-point), ak je to efektívne a architektonicky vhodné (napr. medzi modulom Profil a Message).
- Zdieľané dáta a spoločná identita občana sú centralizované cez modul KKProfile, ktorý slúži ako hlavný referenčný bod pre údaje občana.
- Všetky moduly používajú výhradne REST API volania na sprístupnenie alebo zápis údajov – nie databázové ani súborové integrácie.

Celý systém je navrhnutý v súlade s princípmi distribuovanej architektúry (microservices-like) a umožňuje horizontálne škálovanie jednotlivých častí bez závislosti na centralizovanom integračnom engine.

Zodpovednosť dodávateľa za činnosti súvisiace s ESB

Dodávateľ systému nenesie zodpovednosť za prevádzku, správu ani architektúru ESB vrstvy ako takej – túto zodpovednosť má Objednávateľ (mesto Košice).

Zodpovednosť dodávateľa je nasledovná:

- Definovať požiadavky na VMs
- Definovať požiadavky na potrebné komunikačné kanály (napr. porty, DNS, certifikáty)
- Implementovať a spravovať REST API volania medzi vlastnými modulmi
- Zabezpečiť bezpečnosť a správnosť dátovej komunikácie na svojej strane
- Poskytnúť podporu pri konfigurácii komunikácie s infraštruktúrou mesta

- Spolupracovať s Objednávateľom pri testovaní a overovaní konektivity

Všetky úlohy súvisiace so sieťovou, bezpečnostnou a technickou konfiguráciou prostredia ESB (vrátane nastavenia firewallov, proxy, routovania a dostupnosti VM) sú plne v réžii Objednávateľa.

Integrácia v rámci systému Konto Košičana je zabezpečená cez REST API architektúru nad infraštruktúrnou vrstvou postavenou na komponentoch Orange Cloudu. Neexistuje centralizovaný middleware – jednotlivé moduly komunikujú buď cez túto infraštruktúru, alebo výnimočne priamo medzi sebou. Zodpovednosť za samotnú ESB vrstvu a jej prevádzku nesie mesto Košice, pričom Dodávateľ plní integračné a koordinačné úlohy výhradne na aplikačnej úrovni.

4. Otázka:
V dokumente „Príloha_7a_SP_Specifikacia_predmetu_Zmluvy_Priloha_c._1_k_Zmluve)“ nie je jednotným spôsobom a spoľahlivo určené, či má byť konkrétna požiadavka implementovaná ako webová obrazovka, mobilný prvok, API služba, alebo systémová funkcionalita bez rozhrania. Preto žiadame verejného obstarávateľa o jednoznačné a úplné vyjadrenie k nasledovnému:

Má každá jednotlivá požiadavka (IDKP_xxx) presne určenú cieľovú platformu (web / mobil / API)? Ak áno, prosíme uviesť, kde presne je táto informácia uvedená (napr. názov stĺpca, formát, pravidlo). Ak nie všetky požiadavky túto informáciu obsahujú alebo sú formulované nejednoznačne, žiadame o sprístupnenie súhrnnej tabuľky, v ktorej bude pre každú požiadavku uvedené: cieľová platforma (web, mobil, API), typ komponentu (napr. GUI obrazovka, REST služba, notifikačný prvok), povaha implementácie (nová funkcionalita vs. rozšírenie existujúcej).

Táto špecifikácia je nevyhnutná pre správny návrh architektúry, ocenenie a dodržanie požiadaviek verejného obstarávateľa v ponuke.

Odpoveď:
Verejný obstarávateľ si dovoľuje uviesť, že požiadavky uvedené v Prílohe č. 7i súťažných podkladov - Katalógu požiadaviek (Príloha č. 9 k Zmluve) sú navrhnuté **v súlade s metodickými princípmi MetaIS** a zohľadňujú požiadavky kladené na projekty verejnej správy financované z fondov EÚ, vrátane architektonickej a funkčnej modularity, ktoré boli posudzované a bude požadované plnenie Zadávateľom výzvy.

K otázke určovania cieľovej platformy (web / mobil / API)

Každá jednotlivá požiadavka je v Katalógu požiadaviek definovaná s určením **modulu**, **oblasti požiadavky** a **kontextu použitia**. Tieto atribúty spoločne určujú:

- **cieľovú platformu**,
- **predpokladaný typ komponentu**,
- a **funkčný zámer** implementácie.

Kde sa táto informácia nachádza:

- **Stĺpec „OBLASŤ POŽIADAVKY“** – informuje o cieľovej platforme alebo rozhraní (napr. *„mobilná aplikácia“*, *„web aplikácia“, „admin web“*, *„služba (service)“*).
- **Stĺpec „MODUL“** – identifikuje funkčný celok, do ktorého požiadavka patrí (napr. *KKNotification*, *KKApplication*, *KKOrder*, atď.).
- **Stĺpec „NÁZOV POŽIADAVKY“** – špecifikuje skrátenú formu funkčnosti, typu používateľa a očakávanou komunikáciou (*API*) resp. interakciou.
- **Stĺpec „DETAILNÝ POPIS POŽIADAVKY“** – špecifikuje detailnejší spôsob použitia, vrátane typu používateľa a očakávanej interakcie resp. komunikácie (*REST API*).

Vzhľadom na návrhový princíp **funkčnej modularity a viacvrstvovej architektúry**, každá požiadavka je **viazaná na modul**, ktorý môže zahŕňať viacero komponentov (frontend, backend, služba a jej rozhranie).

K otázke povahy implementácie:

Katalóg požiadaviek obsahuje novú funkcionalitu, pričom prípadná rozširujúca funkcionalita z pohľadu implementácie vyplýva z dokumentácie existujúceho riešenia – konkrétne z príloh obsahujúcich DNR a OpenAPI špecifikácie, ku ktorým má uchádzač prístup. Tieto podklady slúžia na pochopenie existujúceho stavu a umožňujú navrhnúť rozšírenia v súlade s požiadavkami obstarávateľa.

Verejný obstarávateľ považuje poskytnuté informácie, ako aj štruktúru a obsah Katalógu požiadaviek, za dostatočné pre riadne uchopenie predmetu zákazky, návrh architektúry a spracovanie relevantnej cenovej ponuky zo strany uchádzača.

5. Otázka:
V dokumente „vysvetlenie súťažných podkladov č.2“ odpovedá verejný obstarávateľ na 15. otázku ohľadom nezrovnalostí v katalógu požiadaviek. V odpovedi nám nebola jasná podstatná časť otázky – zlé priradenie požiadaviek k modulom. Napr. autentifikácia a registrácia patria skôr do modulu KKAuth, nie KKApplication, čo odpoveď nijako nevysvetľuje. Nie je vykonaná žiadna analýza podobných požiadaviek. Príklad: IDKP_1 a IDKP_2 majú rovnakú oblasť aj podobný význam, ale odpoveď je nejasná, tvrdením, že „nie sú duplicitné“, bez preukázania dôvodu. Neobjasňuje, ako sa má uchádzač vysporiadať s potenciálnou redundanciou. Ak sa má rovnaká funkcionalita implementovať vo viacerých moduloch, mal by to objednávateľ výslovne označiť ako zámer.

Preto žiadame verejného obstarávateľa o jednoznačné vyjadrenie k nasledovnému:
Aké pravidlo platí pre priraďovanie požiadaviek k modulom? Napr. prečo je požiadavka na autentifikáciu uvedená pod modulom KKApplication, a nie pod modulom KKAuth?

Prosíme o zoznam všetkých požiadaviek, ktoré sa týkajú rovnakých funkcionalít (napr. registrácia, prihlásenie, odhlásenie, deaktivácia účtu) s vyznačením:

- či ide o samostatné funkcionality,
- alebo viacnásobný výskyt tej istej požiadavky,
- ak sa líšia len formálne (napr. popisom), ako má uchádzač postupovať – implementovať raz alebo viackrát?

Odpoveď:
Verejný obstarávateľ doplňuje svoju predchádzajúcu odpoveď č.15 a č.13 vo Vysvetlení súťažných podkladov č. 2 nasledovne:

Priraďovanie požiadaviek k modulom

Požiadavky v Prílohe č. 7i – Katalóg požiadaviek (Príloha č. 9 k Zmluve) sú priradené k modulom na základe:

- **primárnej funkčnej alebo procesnej zodpovednosti** za danú oblasť,
- **užívateľského alebo systémového vstupného bodu**, cez ktorý sa funkcionalita vykonáva,
- **pôvodného účelu a logického zaradenia v rámci architektúry riešenia**.

Moduly v rámci navrhovaného riešenia predstavujú **samostatné funkčné celky**, ktoré sú **navzájom prepojené, môžu využívať funkcionality iných modulov** a môžu byť využívané v rôznych aplikáciách (web, mobilná aplikácia, admin portál).

Z tohto dôvodu je pri ich implementácii nevyhnutné zvoliť taký realizačný prístup, ktorý umožní odovzdávanie **plne funkčných a logicky uzavretých celkov**, pričom moduly môžu na svoje korektné fungovanie vyžadovať spoluprácu s inými modulmi a **využívať ich zdieľané alebo opakovane použiteľné komponenty**.

Katalóg funkčných požiadaviek boli vypracované **v súlade s metodickými odporúčaniami a štruktúrou definovanou v MetaIS**, a to najmä podľa požiadaviek kladených na projekty verejnej správy, vrátane štandardov ISVS a architektonického rámca eGovernmentu.

Vyhodnotenie zdanlivej duplicity

Objednávateľ si **nie je vedomý výskytu duplicít v inom rozsahu**, ako je prirodzené pri kooperácii viacerých modulov a aplikácií, ktoré majú zabezpečiť komplexnú funkcionalitu systému. Tento princíp sa prirodzene prejavuje aj v Katalógu požiadaviek, kde sa niektoré funkcionality môžu opakovane vyskytovať – nie však ako duplicita, ale ako **nevyhnutná súčasť spolupracujúcich modulov a aplikácií**, ktoré danú funkcionalitu **používajú v rôznych kontextoch a vrstvách**.

Príklady a analýza: registrácia, autentifikácia, deaktivácia konta

Verejný obstarávateľ analyzoval požiadavky súvisiace s:

- registráciou,
- prihlásením,
- deaktiváciou účtu

Relevantné požiadavky sú uvedené v nasledovnej tabuľke (výber):

ID požiadavky	**Názov požiadavky**	**Modul**	**Oblasť požiadavky**	**Poznámka**/Detailný popis požiadavky
IDKP_1	Konfigurácia mobilnej aplikácie	KKApplication	Registrácia a integrácia aplikácii do ekosystému Konta Košičana	**Zameraná na registráciu mobilnej aplikácie do ekosystému.** „Ako servis chcem sa zaregistrovať do ekosystému KK za pomoci administrátorov Mesta Košíc, získať aplikačné id a oprávnenia mobilnej aplikácie pre registráciu, prihlasovanie a odhlasovanie občana Kontom Košičana. Konfiguračné nastavenia z Azure B2C ténantu mi poskytne administrátor KK.“
IDKP_2	Integrácia mobilnej aplikácie do ekosystému Konta Košicana	KKApplication	Registrácia a integrácia aplikácii do ekosystému Konta Košičana	**Zameraná na konfiguráciu mobilnej aplikácie do ekosystému.** „Ako servis chcem sa integrovať konfiguračné nastavenia integrovať do REST komunikácie. Konfiguračné nastavenia z Azure B2C ténantu mi poskytne administrátor KK.“

IDKP_3	Deaktivácia konta (admin)	KKAuthentication	Administrácia KK	**Funkcionalita pre administrátorov.** „Ako administrátor chcem vedieť deaktivovať KK na základe overovacích údajov občana z Konta Košičana z administrátorského prostredia“
IDKP_4	Deaktivácia konta (občan)	KKAuthentication	Registrácia a autentifikácia KK	**Používateľská deaktivácia vo web aplikácii.** „Ako občan si chcem vedieť deaktivovať svoje konto po prihlásení sa do **webovej** aplikácie Konta Košičana. Po deaktivácie občan stratí možnosť prihlásenia sa do web a mobilných aplikácii umožňujúcich prihlasovanie pomocou KK. Pre opätovnú aktiváciu je nutné nová registrácia.“
IDKP_5	Deaktivácia konta cez web	KKAuthentication	Registrácia a autentifikácia KK	**Používateľská deaktivácia v mobilnej aplikácii.** „Ako občan si chcem vedieť deaktivovať svoje konto po prihlásení sa do **mobilnej** aplikácie Konta Košičana. Po deaktivácie občan stratí možnosť prihlásenia sa do web a mobilných aplikácii umožňujúcich prihlasovanie pomocou KK. Pre opätovnú aktiváciu je nutné nová registrácia.“

Každá z týchto požiadaviek má iný kontext (rola používateľa, rozhranie, cieľ použitia) a je preto vedená ako **samostatná požiadavka**, aj keď technická implementácia môže využívať spoločné komponenty.

Priradenie požiadaviek k modulom nie je striktne technickým rozhodnutím, ale zohľadňuje funkčný, procesný aj používateľský kontext. Každá požiadavka bola definovaná s cieľom zabezpečiť úplné pokrytie očakávanej funkcionality riešenia.

6. Otázka:
V dokumente „Priloha_7i_SP_Katalog_poziadaviek_(Priloha_c._9_k_Zmluve).xlsx“ sa nachádzajú viaceré požiadavky formulované ako tzv. user stories bez akceptačných kritérií alebo bez bližšej špecifikácie požadovaného správania systému.
Príklad: „Ako modul KKOrder chcem vedieť automaticky prepočítať dane za platobné položky.“

V tomto a podobných prípadoch nie je zrejmé:

- aký vstup má byť do funkcionality zadávaný (manuálne, systémovo?),
- aký je výstup a vo forme akého rozhrania (zobrazenie, logovanie, výstup do iného modulu?),
- čo presne znamená „vedieť prepočítať“ z pohľadu implementácie (má modul len vykonať výpočet, má ho aj zobraziť, odoslať niekam?),

- či ide o povinnú funkcionalitu alebo len logickú informáciu o schopnosti systému.

Žiadame verejného obstarávateľa o nasledovné doplňujúce informácie:

Poskytnutie akceptačných kritérií alebo technických špecifikácií k požiadavkám, ktoré sú formulované len v štýle „chcem vedieť“, „chcem byť informovaný“, „chcem získať prehľad“ a podobne, pričom nie je uvedený vstup, výstup ani očakávané správanie systému.

Ak má byť návrh týchto požiadaviek ponechaný na dodávateľa, žiadame potvrdiť:

- návrh riešenia zo strany uchádzača bude predmetom akceptácie zo strany verejného obstarávateľa,
- návrh musí byť súčasťou ponuky alebo až predmetom analýzy po podpise zmluvy,
- požiadavky nebudú počas realizácie spochybňované ako nedodané, ak neboli špecifikované jednoznačne v súťažných podkladoch.

Odpoveď:
Požiadavky formulované ako *user stories* predstavujú zámerové funkcionality, ktoré majú byť predmetom detailnej analýzy po uzatvorení zmluvy. Ich aktuálna formulácia je v súlade s princípmi agilného prístupu a bola zvolená s cieľom ponechať priestor na odborný návrh zo strany dodávateľa a zohľadniť špecifiká technologického riešenia.

Požiadavky formulované ako *user stories* budú predmetom ďalšej analýzy a technického návrhu Dodávateľa po uzatvorení zmluvy. Tento návrh bude podliehať akceptácii Objednávateľa. Akceptačné kritériá budú spoločne dohodnuté a slúžiť ako objektívny základ pre posúdenie splnenia požiadaviek. Tento prístup je v súlade s metodikou riadenia IT projektov a zároveň rešpektuje požiadavky na právnu istotu a kontrolovateľnosť v rámci ESIF projektov.

Zodpovednosť za návrh riešenia

- Návrh konkrétneho riešenia jednotlivých požiadaviek je v kompetencii Dodávateľa.
- Tento návrh bude podrobený **posúdeniu a akceptácii zo strany Objednávateľa** v rámci fázy **Analýzy**, ktorá je integrálnou súčasťou realizácie predmetu zákazky.
- Súčasťou Analýzy bude aj **doprecizovanie akceptačných kritérií**, ktoré Dodávateľ predloží na schválenie Riadiacemu výboru projektu.

Vzťah k predloženiu ponuky a súťažnému konaniu

- Detailný návrh riešenia, ako aj úplné technické špecifikácie nie sú požadované ako súčasť ponuky.
- Uchádzači predkladajú ponuku na základe zadania uvedeného v súťažných podkladoch, pričom detailné parametre implementácie budú rozpracované až po uzatvorení zmluvy.
- Tento prístup je plne v súlade s pravidlami verejného obstarávania aj s pravidlami čerpania z ESIF, keďže zabezpečuje transparentnosť, ale zároveň ponecháva priestor na optimalizáciu riešenia počas realizačnej fázy.

Právna istota v procese akceptácie a kontroly dodania

- Požiadavky, ktoré budú počas Analýzy doplnené o akceptačné kritériá a technické špecifikácie, budú následne záväzne slúžiť ako základ pre overenie riadneho dodania diela.
- Prístup Objednávateľa zabezpečuje dodržanie princípov transparentnosti, primeranosti a proporcionality, ako aj elimináciu rizika neuznania oprávnenosti výdavkov zo strany riadiaceho orgánu ESIF.

Verejný obstarávateľ kladie dôraz na výber takého riešenia, ktoré zabezpečí nielen plnú funkčnosť požadovaného systému, ale zároveň bude spĺňať vysoké nároky na jeho bezpečnosť, stabilitu a dlhodobú udržateľnosť.

V tejto súvislosti je požadované, aby navrhované riešenie:

- bolo technologicky otvorené a flexibilné,
- umožňovalo budúci rozvoj a rozširovanie funkcionalít bez potreby rozsiahlych zásahov do jadra systému,
- bolo finančne efektívne z hľadiska budúcej prevádzky, podpory a servisovania,
- podporovalo transparentný a udržateľný spôsob správy, integrácie a údržby.

Cieľom verejného obstarávateľa je získať moderné, rozšíriteľné a prevádzkovo udržateľné riešenie, ktoré bude dlhodobo slúžiť svojmu účelu s minimálnymi nákladmi na ďalší rozvoj a údržbu.

Z uvedeného dôvodu **je nevyhnutné, aby uchádzači pri príprave ponuky tieto požiadavky zohľadnili** a v návrhu riešenia zvolili taký prístup, ktorý reflektuje nielen aktuálne funkčné požiadavky, ale aj predpokladaný vývoj systému v čase, a to s dôrazom na efektívnosť a hospodárnosť celkového životného cyklu riešenia.

7. Otázka:
V dokumente Príloha_7a_SP_Specifikacia_predmetu_Zmluvy_(Priloha_c._1_k_Zmluve) sa uvádza, že nefunkčné požiadavky na riešenie sú popísané v kapitolách Požiadavky na výkon a dostupnosť služieb a Architektonické požiadavky.

Vzhľadom na ich zásadný vplyv na návrh architektúry a ocenenie rozsahu riešenia, žiadame o jednoznačné a konkrétne doplnenie alebo výpis nasledovných nefunkčných požiadaviek:

- Dostupnosť systému – aká je požadovaná úroveň dostupnosti v % za mesiac alebo rok (napr. 99,5 %), a či sú súčasťou riešenia aj SLA zmluvne viazané parametre.
- Výkonové parametre a časy odozvy – požadované maximálne odozvy backendových služieb, webového frontendu a mobilného riešenia, ak sú definované.
- Škálovateľnosť riešenia – či sa vyžaduje horizontálne alebo vertikálne škálovanie a v akom objeme/počte súčasne obsluhovaných používateľov.
- Bezpečnostné požiadavky – či sa vyžaduje dodržiavanie konkrétnych bezpečnostných štandardov (napr. ISO/IEC 27001, OWASP Top 10), aké sú požiadavky na šifrovanie údajov v pokoji a v prenose, spôsob autentifikácie a autorizácie (napr. eID, B2C).
- Auditovateľnosť – čo presne má byť auditovateľné, v akej forme majú byť ukladané záznamy (logy), ako dlho sa majú uchovávať a či má byť umožnený externý audit.

Žiadame o explicitné uvedenie týchto parametrov v odpovedi, alebo o presnú lokalizáciu v dokumentácii – vrátane čísel príloh, kapitol a ID požiadaviek, ktoré tieto nefunkčné vlastnosti popisujú.

Odpoveď:
Verejný obstarávateľ si dovoľuje uviesť, že všetky relevantné dokumenty k predmetu zákazky boli sprístupnené v súlade s § 42 zákona č. 343/2015 Z. z. o verejnom obstarávaní a obsahujú dostatočné informácie potrebné na vypracovanie ponuky.

V tejto súvislosti považuje verejný obstarávateľ za potrebné zdôrazniť, že účelom vysvetlenia súťažných podkladov **nie je vykonávanie rešerší alebo vyhľadávanie konkrétnych údajov v dokumentoch**, ktoré boli uchádzačom riadne a úplne poskytnuté.

Zároveň verejný obstarávateľ predpokladá, že **uchádzač má primeranú znalosť** legislatívnych, bezpečnostných a technologických rámcov platných pre projekty verejnej správy a financovaných z fondov EÚ (najmä ESIF), ako aj skúsenosti s návrhom a dodaním riešení pre organizácie verejnej moci (OVM).

V prípade, že niektoré z ustanovení súťažných podkladov budú po ich dôslednom preštudovaní naďalej vnímané ako nejednoznačné alebo protichodné, verejný obstarávateľ je pripravený ich vysvetliť v intenciách zákona.

Tabuľka parametrov:

Príloha 7a - Príloha_7a_SP_Specifikacia_predmetu_Zmluvy_(Priloha_c._1_k_Zmluve).docx
Príloha 7i - Príloha_c._7i_- Katalóg požiadaviek (Príloha č. 9 k Zmluve).xlsx

Príloha	Kapitola	ID Požiadavky	Popis Požiadavky	Poznámka
Príloha 7a Príloha 7i	2.7	IDKP_253	Požiadavka na dostupnosť služieb…	Dostupnosť systému
Príloha 7a Príloha 7i	2.7	IDKP_250	Požiadavka na odozvu služieb pri testovaní záťaže systému	Výkonové parametre a časy odozvy
Príloha 7i		IDKP_315	RTO (Recovery Time Objective)	Dostupnosť systému
Príloha 7i		IDKP_316	RPO (Recovery Point Objective)	Dostupnosť systému
Príloha 7a Príloha 7i	2.5	IDKP_292	Požiadavky na implementáciu a vývoj diela	Auditovateľnosť, stav a chyby servisov, Štruktúru dodá Objednávateľ po podpise zmluvy. Uchovávanie logov je na strane Objednávateľa.
Príloha 7a Príloha 7i	2.5	IDKP_289	Požiadavka na zohľadnenie „best practice“	Škálovateľnosť riešenia
Príloha 7a Príloha 7i	2.3	IDKP_265	Vyhláška č. 78/2020 Z. Z. – Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o štandardoch pre informačné technológie verejnej správy	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_266	Zákon č. Č. 305/2013 Z. Z. O elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_269	Aproximačné nariadenia vlády SR – Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_270	Aproximačné nariadenia vlády SR – Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov,	Legislatívne a bezpečnostné požiadavky

			ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)	
Príloha 7a Príloha 7i	2.3	IDKP_271	Zákon č. 18/2018 Z. Z. O ochrane osobných údajov a o zmene a doplnení niektorých zákonov.	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_272	Zákon č. 69/2018 Z. Z. O kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_273	Zákon č. 272/2016 Z. Z. O dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov v znení neskorších predpisov.	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_274	Zákon č. 95/2019 Z. Z. O informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov. Je požadované, aby jednotlivé IS boli vyvinuté formou open-source (EUPL licenčný model).	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_275	Metodika merania dátovej kvality vo verejnej správe MIRRI (ÚPVII) (dostupná na https://datalab.digital/wp-content/uploads/Metodika-merania-dátovej-kvality-vo-verejnej-správe.pdf)	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_276	Metodické usmernenie Úradu podpredsedu vlády SR pre investície a informatizáciu č. 3639/2019/oDK-1 o postupe zaraďovania referenčných údajov do zoznamu referenčných údajov vo väzbe na referenčné registre a vykonávania postupov pri referencovaní (dostupný na https://datalab.digital/wp-content/uploads/Metodické-usmernenie-ÚPVII-č.-3639-2019-oDK-1-FINAL-1.pdf)	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_277	Vyhláška č. 85/2020 Z. Z.– Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu o riadení projektov	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_278	Vyhláška č. 179/2020 Z. Z. – Vyhláška Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, ktorou sa ustanovuje spôsob kategorizácie a obsah bezpečnostných opatrení informačných technológií verejnej správy	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_279	Vyhláška Úradu na ochranu osobných údajov č. 158/2018 Z. Z. O postupe pri posudzovaní vplyvu na ochranu osobných údajov.	Legislatívne a bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.3	IDKP_279	Súvisiace strategické dokumenty: 1. Národná koncepcia informatizácie verejnej správy Slovenskej republiky (NKIVS), kde sa definuje vízia, strategické ciele a smery e-Governmentu v SR, 2. Strategická priorita Multikanálový prístup 3. Pravidlá publikovania elektronických služieb do multikanálového prostredia verejnej správy 4. Reformný zámer Koncepčné budovanie digitálnej a inovatívnej VS	Legislatívne a bezpečnostné požiadavky

			Dostupné na: https://www.mirri.gov.sk/sekcie/strategicke-priority-nikvs/index.html	
Príloha 7a Príloha 7i	2.4	IDKP_281	Bezpečnostné požiadavky a požiadavky na vykonanie penetračného testovania, vrátane overenia súladu diela s bezpečnostnými požiadavkami špecifikované v Metodike pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (dostupná na https://www.csirt.gov.sk/wp-content/uploads/2021/07/MetodikaZabezpeceniaIKT_v2.1-1.pdf?csrt=6865556012032554954)	Bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.4	IDKP_282	Požiadavka na súlad a primerané aplikovanie OWASP Metodika pre REST SaaS API - https://wiki.owasp.org/index.php/OWASP_SaaS_Rest_API_Secure_Guide.	Bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.4	IDKP_283	Požiadavka na odstránenie nedostatkov penetračného testovania a realizáciu diela v súladu s bezpečnostnými požiadavkami špecifikované v Metodike pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti (dostupná na https://www.csirt.gov.sk/wp-content/uploads/2021/07/MetodikaZabezpeceniaIKT_v2.1-1.pdf?csrt=6865556012032554954)	Bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.4	IDKP_284	Požiadavky na súčinnosť pri vykonaní nezávislého bezpečnostného auditu vrátane auditu zdrojového kódu dodaných komponentov alebo aplikácii a penetračných testov v rozsahu činností, ktoré vykoná Objednávateľom určený subjekt: 1. Vykonanie auditu komponentov, ktoré sú výstupom plnenia diela. 2. Štruktúrovaný popis nálezov auditu vo formáte XLS s prioritizáciou a návrhom riešenia. Overenie zapracovanie pripomienok a odstránenia nálezov brániacich riadnemu používaniu predmetu diela.	Bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.4	IDKP_285	Vyhláška č. 164/2018 Z. Z. – Vyhláška NBÚ SR, vyhláška o IKPS, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby) v platnom znení.	Bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.4	IDKP_286	Vyhláška č. 165/2018 Z. Z. – Vyhláška NBÚ SR, vyhláška o KBI, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov v platnom znení.	Bezpečnostné požiadavky
Príloha 7a Príloha 7i	2.4	IDKP_287	Vyhláška č. 362/2018 Z. Z. – Vyhláška NBÚ SR, vyhláška o OBO, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení v platnom znení.	Bezpečnostné požiadavky
Príloha 7a	2.1	IDKP_x04	Servisy a aplikácie musia používať/integrovať existujúcu jednotnú autentifikáciu a autorizáciu Konta Košičana prostredníctvom Azure AD B2C (OpenID Connect, OAuth2, JWT), MK-KKaKES-DNR-PR-10-Integrácia-Azure B2C-Integračný manuál.docx.	Bezpečnostné požiadavky

8. Otázka:
Žiadame verejného obstarávateľa o vysvetlenie, prečo sú v dokumente Príloha_7b_SP_Podrobna_cenova_kalkulacia_(Priloha_c._2_k_Zmluve) pevne stanovené počty jednotiek (človekodní) jednotlivých expertov pri stanovení návrhu ceny, resp. či je možné s týmito počtami v ponuke hýbať. Nemal by mať uchádzač možnosť tieto jednotky meniť podľa vlastného zhodnotenia prácnosti jednotlivých expertov?

Odpoveď:
Prácnosť expertov bola stanovaná na základe výzvy a to formou CBA analýzy dodanej k výzve, ktorá stanovila výšku ceny projektu. Verejný obstarávateľ nevidí problém s uvoľnením údajov a uvoľní ich. Verejný obstarávateľ zverejnil Prílohu č. 7b Podrobná cenová kalkulácia (Príloha č. 2 k Zmluve) oprava č. 1, v ktorej odomkol bunky.

V Košiciach, dňa 07.08.2025
Spracoval: JUDr. Martin Šustrík na základe podkladov Referátu správy aplikácií