MESTO KOŠICE

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

Spis č.: MK/A/2025/19238

Vysvetlenie súťažných podkladov č. 5

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 31.07.2025 poskytujeme nasledovnú odpoveď:

1. Otázka:
Ako je požadované určiť kategorizáciu informačného systému podľa zákona č. 69/2018 Z.z.?

(IDKP272, IDKP285, IDKP286)_
V požiadavke sa uvádza povinnosť dodržiavať zákon o kybernetickej bezpečnosti, ale nie je uvedené, či má byť systém kategorizovaný ako základná služba, významná služba alebo digitálna služba. Táto klasifikácia má zásadný vplyv na rozsah bezpečnostných opatrení a povinnosti voči NBÚ.
Príklad: Ak ide o základnú službu, je potrebné zabezpečiť auditovateľnosť, hlásenie incidentov a súlad s vyhláškou č. 362/2018 Z.z. Prípadne definujte presnejšie.

Odpoveď:
Mesto Košice je už v súčasnosti poskytovateľom základnej služby v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti. V rámci tejto pozície pravidelne vykonáva bezpečnostné audity a plní zákonné povinnosti.
Ekosystém „Konto Košičana“ je dlhodobo vyvíjaný ako súčasť tejto infraštruktúry a je kategorizovaný ako základná služba. Z toho vyplýva, že na systém sa vzťahujú všetky povinnosti poskytovateľa základnej služby v zmysle zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti, vrátane súladu s vyhláškou č. 362/2018 Z. z..

2. Otázka:
Ako je požadované navrhnúť bezpečnostné zóny medzi on-premise infraštruktúrou mesta a Azure cloudom – má ísť o segmentáciu podľa úrovne dôvery, alebo podľa funkčných modulov?

(IDKPx09, IDKP292)
Požiadavka definuje hybridnú architektúru, ale nešpecifikuje, ako má byť navrhnutá segmentácia medzi cloudom a mestskou infraštruktúrou. Nie je jasné, či sa očakáva použitie DMZ, VPN, privátnych peeringov alebo iných mechanizmov.
Príklad: Má byť modul KKAuthentication v Azure oddelený od KKProfile v on-premise cez VPN tunel, alebo sa očakáva použitie Azure ExpressRoute? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy. Súčasné riešenie je v prílohách - Príloha č. 9 SP - Technická dokumentácia – Konto Košičana (súčasný stav), dokument MK-KKaKES-DNR-PR-02-Autentifikacia.docx – stať Technologická architektúra.

3. Otázka:
Ako je požadované spravovať tajomstvá (napr. API kľúče, tokeny, certifikáty) – má sa použiť centralizovaný vault, alebo je akceptovaná distribúcia v rámci CI/CD?

(IDKP292, IDKP264)
Nie je uvedené, kde a ako majú byť tajomstvá uložené, rotované a auditované. Bez tejto špecifikácie hrozí riziko úniku citlivých údajov alebo nedostatočnej kontroly nad prístupmi.
Príklad: Je akceptované použitie Azure Key Vault s RBAC, alebo sa očakáva iné riešenie ako HashiCorp Vault? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy. Zákon o verejnom obstarávaní nám neumožňuje určovať konkrétne produkt, pokiaľ nejde o existujúci stav. Mesto momentálne nemá centralizovaný vault. Súčasné riešenie využíva v prípade mestskej infraštruktúry formou distribúcie v rámci CI/CD, v Azure cloude pomocou environment variables a v prípade AD B2C jeho službami.

4. Otázka:
Ako je požadované zabezpečiť REST API rozhrania pred zneužitím – je požadovaný rate limiting, throttling, alebo iné mechanizmy ochrany?

(IDKPx01, IDKPx06, IDKP189, IDKP190)
Požiadavky definujú API-First prístup, ale neobsahujú informácie o ochrane pred nadmerným volaním, DoS útokmi alebo zneužitím API. Nie je jasné, či sa očakáva použitie API Gateway alebo iných bezpečnostných vrstiev.
Príklad: Má byť súčasťou riešenia ochrana cez JWT validáciu, IP whitelisting alebo dynamické throttling pravidlá? Prípadne definujte presnejšie.

Odpoveď:
Integračnú vrstvu momentálne tvorí ESB vrstva infraštruktúry mesta v správe mesta Košice, teda aj ochrane proti zneužitiu na tejto vrstve je na strane mesta. S API GW ako technologickou platformou sa v tomto projekte neráta. Samozrejme pre komunikáciu občana a administrátorov so servismi ako komunikácia aplikácii medzi sebou je už v súčasnosti zabezpečená pomocou autorizácie (OIDC, oAuth2, JWT) popísaných v prílohách o súčasnom stave MK-KKaKES-DNR-PR-02-Autentifikacia.docx, MK-KKaKES-DNR-PR-05-Autentifikacia-Aplikacii.docx a MK-KKaKES-DNR-PR-10-Integrácia-Azure B2C-Integračný manuál.docx. Je vyžadované aby API bolo zabezpečené týmito autorizačnými prostriedkami.

5. Otázka:
Ako je požadované zabezpečiť dôvernosť obsahu push notifikácií a e-mailov – môžu obsahovať osobné údaje, alebo musia byť anonymizované?

(IDKP21, IDKP43, IDKP44, IDKP45)
Nie je špecifikované, aký typ údajov môže byť zasielaný v notifikáciách. Nie je jasné, či je prípustné zasielať konkrétne osobné údaje alebo len všeobecné upozornenia.
Príklad: Je prípustné zaslať notifikáciu „Vaša daň z nehnuteľnosti je splatná do 31.3.2025“ alebo len „Máte novú správu v konte“? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy, pričom je požadované dodržiavanie zásad GDPR.

6. Otázka:
Ako je požadované zabezpečiť QR kódy používané na identifikáciu – majú byť kryptograficky podpísané, časovo obmedzené alebo jednorazové?

(IDKP74–IDKP76, IDKP151)_

Požiadavky popisujú použitie QR kódov, ale neuvádzajú bezpečnostné parametre ako platnosť, podpis alebo ochranu pred zneužitím. Nie je jasné, či sa majú QR kódy generovať dynamicky a ako sa má overovať ich platnosť.
Príklad: Má QR kód obsahovať JWT token s expiráciou 5 minút a podpisom privátnym kľúčom mesta? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy

7. Otázka:
Ako je požadované zabezpečiť ochranu údajov v offline režime mobilnej aplikácie – majú byť šifrované, alebo sa má offline režim zakázať?

(IDKP12, IDKP25–IDKP33)_
Nie je uvedené, či aplikácia podporuje offline režim a ako sa majú chrániť lokálne uložené údaje. Ak sa offline režim povoľuje, je potrebné špecifikovať, aké údaje môžu byť uložené a akou formou.
Príklad: Má byť použité šifrované úložisko s biometrickým prístupom, alebo sa má offline režim obmedziť len na neosobné dáta? Prípadne definujte presnejšie.

Odpoveď:
Offline režim mobilnej aplikácie nie súčasťou katalógu požiadaviek, teda nebude riešený.

8. Otázka:
Ako je požadované zabezpečiť ochranu údajov v podnetoch občanov – najmä pri nahrávaní fotografií a lokalizačných údajov?

(IDKP77–IDKP86, IDKP94, IDKP99)
Podnety môžu obsahovať osobné údaje, fotografie osôb, GPS súradnice. Nie je uvedené, ako sa majú tieto dáta šifrovať, anonymizovať alebo validovať pred uložením.
Príklad: Má byť fotografia automaticky anonymizovaná (rozmazanie tvárí, ŠPZ), alebo sa to ponecháva na používateľa? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy, pričom je požadované dodržiavanie zásad GDPR. Podnety majú obsahovať identifikátor Konta Košičana, anonymizácia by mala byť na strane občana a validácia na strane mesta.

9. Otázka:
Ako je požadované zabezpečiť ochranu údajov pri spracovaní platobných údajov – má byť riešenie v súlade s PCI-DSS, alebo sa všetko deleguje na PSP?

(IDKP110–IDKP117, IDKP130–IDKP133)
Nie je uvedené, či má byť dodávateľ PCI-DSS compliant, alebo sa všetky platby realizujú cez tretie strany. Táto informácia je kľúčová pre návrh architektúry a zodpovednosti.
Príklad: Má byť platobná brána integrovaná cez iframe (bez spracovania údajov na strane mesta), alebo sa očakáva vlastné spracovanie? Prípadne definujte presnejšie.

Odpoveď:
Mesto nemá záujem byť PSP, avšak riešenie má byť v súlade s PCI-DSS a PSP musí byť oprávnený poskytovať platobné služby v súlade s platnou legislatívou SR a EÚ. Návrh riešenia je na strane Dodávateľa a vo fáze Analýzy, bude posúdený a schválený Odberateľom. Integrácia platobnej brány má však spĺňať katalógové požiadavky na moduly KKMarketplace, KKOrder, KKPayment a KKBilling.

10. Otázka:
Ako je požadované zabezpečiť ochranu údajov pri správe kariet (napr. ZŤP, rezidentské, MHD) – majú byť vizuálne chránené (napr. watermark), alebo len prístupovo?

(IDKP90–IDKP98)
Nie je uvedené, ako sa majú tieto údaje zobrazovať a chrániť pred zneužitím. Nie je jasné, či sa majú používať vizuálne ochranné prvky alebo len prístupová kontrola.
Príklad: Má byť karta ZŤP zobrazovaná s QR kódom a časovou platnosťou, alebo ako statický obrázok? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy.

11. Otázka:
Ako je požadované zabezpečiť ochranu údajov pri správe personalizovaných kalendárov – sú tieto údaje považované za osobné a ako sa majú chrániť?

(IDKP60, IDKP66, IDKP69–IDKP73)
Kalendáre môžu obsahovať dáta o splatnosti daní, podujatiach, ktoré sa týkajú konkrétneho občana. Nie je uvedené, či sa majú tieto údaje šifrovať alebo len filtrovať podľa prístupových práv.
Príklad: Má byť kalendár synchronizovaný s externým kalendárom (napr. Google Calendar) a ak áno, ako sa zabezpečí ochrana údajov? Prípadne definujte presnejšie.

Odpoveď:
Občan má vedieť pristúpiť ku svojim údajom na základe prístupových práv. Požiadavka na synchronizáciu dát nie je v katalógu požiadaviek. Občan si však má možnosť pridať kalendárové udalosti do svojho kalendára pomocou protokolu iCal zo svojej mobilnej aplikácie IDKP_61, IDKP_207.

12. Otázka:
Ako je požadované zabezpečiť ochranu údajov pri správe zliav a klasifikácie občanov – sú tieto údaje považované za citlivé?

(IDKP107, IDKP127)
Zľavy môžu byť viazané na sociálny status, zdravotný stav alebo iné citlivé atribúty. Nie je uvedené, ako sa tieto údaje majú spracúvať a zobrazovať.
Príklad: Má byť zľava „ZŤP 50 %“ viditeľná v profile občana, alebo len ako anonymizovaný benefit? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy, pričom je požadované dodržiavanie zásad GDPR.

13. Otázka:
Ako je požadované zabezpečiť ochranu biometrických údajov pri autentifikácii – sú tieto údaje spracúvané lokálne alebo centrálne?

(IDKP9, IDKP111)
Nie je uvedené, či sa biometria (napr. FaceID, odtlačok prsta) spracúva len na zariadení, alebo sa prenáša do backendu. Táto informácia je kľúčová z pohľadu GDPR a bezpečnosti.

Príklad: Je akceptované použitie len natívneho biometrického API systému (napr. Android BiometricPrompt), alebo sa má biometria validovať aj server-side? Prípadne definujte presnejšie.

Odpoveď:
Návrh riešenia je v kompetencii Dodávateľa, v zmysle ustanovenia bodu 4.35 zmluvy. Zákon o verejnom obstarávaní nám neumožňuje určovať konkrétne produkt, pokiaľ nejde o existujúci stav.

14. Otázka:
Ako je požadované zabezpečiť bezpečnosť pri interakcii s aplikáciami tretích strán – napr. pri presmerovaní z kariet, kalendárov alebo identifikácie?

(IDKP92, IDKP97, IDKP63, IDKP68, IDKP75)_
Nie je uvedené, či sa majú používať bezpečnostné tokeny, šifrovanie, alebo iné mechanizmy pri prechode medzi systémami. Nie je jasné, ako sa má zabezpečiť dôveryhodnosť a integrita údajov pri presmerovaní.
Príklad: Má byť presmerovanie realizované cez signed URL s časovou platnosťou, alebo je akceptované jednoduché HTTP presmerovanie? Prípadne definujte presnejšie.

Odpoveď:
Interakcia v rámci systémov Odberateľa má byť realizovaná prostredníctvom autorizovaného REST API. V prípade presmerovaní do aplikácii tretích strán mimo systémov Odberateľa, Dodávateľ nerieši bezpečnosť ide len HTTP presmerovanie/zobrazenie aplikácie tretej strany.

15. Otázka:
Vzhľadom na to, že predmet zákazky obsahuje len vývoj systému na základe presného zadania (napr. formou MD), pričom fáza jeho následnej prevádzky, podpory a údržby má byť podľa tohto predpokladu obstarávaná osobitne v samostatnej zákazke, chceli by sme požiadať o objasnenie, ako je zabezpečené:
-že nejde o účelové rozdelenie zákazky, ktoré by mohlo byť v rozpore s § 10 zákona o verejnom obstarávaní a so zásadou hospodárnosti pri použití verejných prostriedkov,
-že v prípade následnej súťaže na prevádzku bude zabezpečený skutočný rovný prístup všetkých uchádzačov – najmä vzhľadom na fakt, že systém bude dodaný „na mieru“ a jeho technické prevzatie iným subjektom bez prístupu k zdrojovému kódu, know-how a dokumentácii býva v praxi prakticky nemožné,
-že plánované riešenie je v súlade s pravidlami oprávnenosti výdavkov eurofondových projektov, najmä vo vzťahu k zabezpečeniu povinnej udržateľnosti projektu, ktorá má byť financovaná mimo pôvodného rozpočtu.

Zároveň si dovoľujeme upozorniť, že takéto rozdelenie môže v praxi viesť k neprimeranej konkurenčnej výhode pôvodného dodávateľa vývoja, ktorý si môže kompenzovať cenu za dodanie systému v následnej súťaži na prevádzku – čím sa narúša princíp rovnakého zaobchádzania.

Prosíme o stanovisko obstarávateľa k vyššie uvedeným bodom, vrátane informácie, ako je zabezpečená transparentnosť, hospodárnosť a nediskriminačný prístup v plánovanom postupe.

Odpoveď:
Rozdelenie zákazky na vývoj systému a jeho následnú prevádzku je vecne odôvodnené – ide o odlišné typy plnenia, realizované v rôznych fázach projektu. Nejde o účelové rozdelenie zákazky ani o obchádzanie zákona (§ 10 ZVO), ale o zabezpečenie hospodárnosti a flexibility.

Obstarávateľ si je vedomý rizika neprimeranej výhody pôvodného dodávateľa. Preto je v zmluve zabezpečené odovzdanie zdrojového kódu, dokumentácie a práv na ďalší rozvoj systému, ako aj zmluvne zabezpečená prenositeľnosť licencií integrovaných produktov tretích strán. Tým sa umožní rovný prístup v následnej súťaži na prevádzku.

Zároveň upozorňujeme, že v súčasnosti nie je presne definovaný konečný stav systému, ktorý by bol predmetom SLA. Objednávateľ zatiaľ nevie, v akej miere bude riešenie servisovať vlastnými kapacitami a v akom rozsahu bude služby nakupovať.

Zvolený postup je v súlade s pravidlami oprávnenosti výdavkov z NFP, vrátane zabezpečenia udržateľnosti mimo pôvodného rozpočtu. Verejný obstarávateľ stanoví podmienky tak, aby zabezpečil transparentnosť, hospodárnosť a nediskrimináciu v plánovanom postupe verejného obstarávania.

16. Otázka:
V rámci prípravy na účasť v plánovanom verejnom obstarávaní sme testovali aktuálne prevádzkovanú verziu systému Konto Košičana v rôznych prehliadačoch a prostrediach s viacerými členmi nášho tímu. Väčšine z nich sa však nepodarilo úspešne registrovať, alebo prihlásiť do systému, pritom dostali výbmery, majú v meste Košice trvalí pobyt, prípadne narazili na iné technické problémy ako zobrazenie údajov po úspešnom prihlásení, ktoré im znemožnili relevantné otestovanie jeho funkcionality.

Z uvedeného nám vyplýva, že systém aktuálne nie je plne funkčný pre všetkých používateľov, čo môže byť relevantné pre posúdenie jeho kvality, stability a pripravenosti na ďalší rozvoj alebo prebratie iným dodávateľom.

V tejto súvislosti si dovoľujeme požiadať:
- O informáciu, akými testovacími scenármi alebo záťažovými testami aktuálna verzia systému prešla, vrátane rozsahu a výsledkov týchto testov,
- O sprístupnenie relevantnej odbornej dokumentácie k týmto testom, resp. k architektúre riešenia a spôsobu autentifikácie používateľov.

Tieto informácie sú pre nás dôležité z pohľadu posúdenia reálnej stability systému a jeho predpokladov na prevzatie či rozvoj v rámci ďalších fáz projektu.

Odpoveď:
Na základe podnetu si dovoľujeme uviesť, že registračná a prihlasovacia časť systému Konto Košičana je funkčná a bežne využívaná verejnosťou (okolo 10 000 registrovaných občanov). V prípadoch, keď boli zaznamenané problémy s registráciou alebo prihlásením, išlo o individuálne situácie na strane používateľa – napríklad:

- pokus o opakovanú registráciu už existujúceho účtu,
- použitie nesprávneho registračného kódu,
- chybne zadané údaje.

Tieto prípady neboli spôsobené technickou chybou systému.

Systém prešiel interným testovaním vrátane funkčných a integračných testov. Záťažové testy v plnom rozsahu neboli realizované.

K žiadosti o sprístupnenie odbornej dokumentácie k testom, architektúre riešenia a spôsobu autentifikácie používateľov si dovoľujeme uviesť, že dokumentácia k registrácii a autentifikácii používateľov je podľa verejného obstarávateľa v dostatočnom rozsahu súčasťou súťažných podkladov tohto verejného obstarávania.

V Košiciach, dňa 04.08.2025
Spracoval: JUDr. Martin Šustrík na základe podkladov Referátu správy aplikácií