Opis predmetu zákazky

I. Predstavenie kontextu

Cieľom predmetu zákazky je overiť vhodný model zabezpečenia ďalšieho rozvoja a prevádzky systému, identifikovať riziká prevzatia existujúceho riešenia a získať podklady pre nastavenie budúcej verejnej zákazky.

a) Riešenie pozostáva z frontendovej a backendovej časti webovej aplikácie. Využívajú sa moderné technológie - Next.js, NestJS, PostgreSQL. K dispozícii máme pre frontendovú a backendovú časť riešenia:

- popis architektúry (routing medzi komponentami, službami, API a databázami)
- zoznam závislostí a integrácií na tretie strany
- Popis deployment procesu
- členov interného tímu, ktorí vedia v úvode spolupráce poskytnúť onboarding do riešenia

b) Frontend je aplikácia Next.js 14 App Router, ktorá slúži ako webové rozhranie pre interný systém. Je jediným konzumentom backendu NestJS. Používatelia pristupujú k systému prostredníctvom webového prehliadača pre počítače (plnohodnotné rozhranie s bočnou navigáciou).

c) Backend je aplikácia NestJS podporovaná PostgreSQL (prostredníctvom Prisma ORM), MinIO pre ukladanie súborov a Azure AD pre autentifikáciu. Integruje sa s niekoľkými službami SOAP/REST tretích strán.

Cieľom budúcej súťaže je obstarať kompletný tím, ktorý bude ďalej spolupracovať s business ownerom na strane HMBA a pracovať na sprioritizovaných taskoch podľa backlogu. Požadovaný stav je priebežný rozvoj riešenia a zabezpečenie stability prevádzky. Verejný obstarávateľ hľadá takého zmluvného partnera s ktorým bude pravidelne komunikovať a hľadať najvhodnejšie spôsoby riešenia, vzhľadom na to sa verejný obstarávateľ rozhodol neobmedzovať budúceho dodávateľa v spôsobe dosiahnutia cieľa, ale stanoviť požadovanú výslednú kvalitu.

Predmetom zákazky je zabezpečenie:

I. Predstavenie kontextu
II. Prevzatie, audit a stabilizácia riešenia
III. Architektúra a výkonnosť
IV. Prevádzka a incident management
V. Spolupráca, handover a dokumentácia
VI. Personálne zabezpečenie a kontinuita
VII. Záväzky verejného obstarávateľa

II. Prevzatie, audit a stabilizácia riešenia,

Počiatočný audit bude pozostávať minimálne z nižšie popísaných súčastí. Prvé výstupy a odporúčania budú dodané do 10 pracovných dní od sprístupnenia zdrojových kódov, existujúcej dokumentácie a potrebných prístupov. Kompletné výsledky budú prezentované **do 4 týždňov**, formou **odovzdanej dokumentácie**, a tiež stretnutia alebo workshopu s vývojárskym tímom aj zástupcami obstarávateľa. Verejný obstarávateľ poskytne dodávateľovi dostupné podklady potrebné na prevzatie riešenia, najmä zdrojové kódy, dostupnú technickú dokumentáciu, popis architektúry riešenia, zoznam integrácií na tretie strany, popis deployment procesu a dostupné prevádzkové informácie v rozsahu primeranom možnostiam verejného obstarávateľa. V prípade potreby si dodávateľ vyžiada ďalšie podklady alebo súčinnosť nevyhnutnú na riadne vykonanie úvodnej analytickej fázy. Verejný obstarávateľ požaduje aby budúci dodávateľ disponoval kapacitami pre samostatné bezpečnostné posúdenie pokrývajúce aplikačnú aj infraštruktúrnu vrstvu a bol schopný výsledky dodať spolu s technickým auditom bez závislosti na existujúcej bezpečnostnej dokumentácii.

Formát výsledného dokumentu bude ponechaný na dodávateľa, súčasťou úvodného auditu musí byť:

a) **Technický audit** pokrývajúci kvalitu kódu, pokrytie automatizovanými testami, vývojové a nasadzovacie procesy, infraštruktúru, integrácie tretích strán a bezpečnosť závislostí. Výsledkom bude dokument obsahujúci manažérske zhrnutie, technické zistenia s maticou rizík podľa závažnosti, identifikáciu technického dlhu a prioritizovaný plán nápravných krokov. Súčasťou bude aj identifikácia oblastí so zvýšenou závislosťou na nedostatočne zdokumentovaných znalostiach alebo kritických osobných znalostiach.

b) **Prevádzkový audit a stabilizačná roadmapa** - audit infraštruktúry, monitoringu, logovania, spracovania chýb a alertingu začne bezprostredne po prevzatí prístupov. Pri riešeniach s integráciami na tretie strany bude súčasťou posúdenia aj návrh spôsobu rozlíšenia pôvodu incidentov a odporúčanie evidencie incidentov podľa aplikačnej, infraštruktúrnej alebo externej príčiny. Kompletná roadmapa stabilizácie bude dodaná spolu s výsledkami technického auditu. Stabilizačné opatrenia budú navrhnuté ako prioritizované zásahy nevyhnutné na odstránenie identifikovaných rizík bez neprimeraného dopadu na funkčný rozsah alebo dostupnosť riešenia.

c) **Bezpečnostné posúdenie** - pokrýva autentifikáciu a autorizáciu, model rolí a oprávnení, audit logy, šifrovanie dát a bežné aplikačné zraniteľnosti. Výstupom je bezpečnostný report s nálezmi klasifikovanými podľa závažnosti a priorizovanými odporúčaniami. Posúdenie primerane zohľadní aj aktuálnosť používaných technológií a aktualizačný režim kritických komponentov riešenia.

d) **Odporúčanie rozvojovej stratégie** - odporúčanie, či je pre daný systém vhodnejší priebežný rozvoj, čiastočný refaktoring alebo väčší architektonický zásah. Odporúčanie musí byť odôvodnené analýzou technického dlhu, miery závislostí, testovateľnosti, frekvencie incidentov a nákladov na údržbu v porovnaní s nákladmi na zásah, pričom zohľadní strednodobú rozvojovú roadmapu systému. Odporúčanie bude zároveň reflektovať potrebu zachovania kontinuity prevádzky a minimalizácie dopadu navrhovaných opatrení na používateľov systému.

Navrhnutú štruktúru môže dodávateľ ďalej rozšíriť alebo upraviť poľa svojho metodického prístupu.

III. Architektúra a výkonnosť

a) **Odolnosť integračnej vrstvy** - riešenie musí obsahovať mechanizmy zabezpečujúce odolnosť voči krátkodobým aj dlhodobým výpadkom externých integrácií. Tie nesmú spôsobiť úplnú nedostupnosť systému ani kaskádové zlyhanie. Kritické správy v prípade nedostupnosti nesmú byť strácané, ale zachytávané na neskoršie spracovanie. Pre každú kritickú integráciu musí byť definované správanie systému v prípade výpadku. Alerting musí umožniť jasné rozlíšenie zodpovednosti za incident podľa zdroja. Súčasťou návrhu musí byť aj mechanizmus opakovaného spracovania zlyhaných požiadaviek a evidencia neúspešných volaní umožňujúca ich dohľadanie a vyhodnotenie.

b) **Sledovanie a optimalizácia** - riešenie musí obsahovať zdokumentovaný prístup k systematickému sledovaniu nasadeného riešenia, pokrývajúci aplikačnú aj dátovú vrstvu. Musia byť definované sledované metriky, periodicita ich vyhodnocovania a postup optimalizácie s rozlíšením rýchlych opatrení a štrukturálnych zásahov. Monitoring musí pokrývať aj dostupnosť externých integrácií, kapacitné limity a trendy výkonu umožňujúce včasnú identifikáciu degradačných javov. Záťažové testovanie simulujúce produkčné podmienky musí byť súčasťou vývojového procesu.

c) **Migrácia produkčného prostredia** - v prípade nutnosti migrácie produkčných systémov do nového prostredia, musí byť toto realizované ako riadená zmena s paralelnou prevádzkou pôvodného a nového stavu, intenzívnym monitoringom a vopred pripraveným a otestovaným rollback plánom. Musia byť definované jasné rozhodovacie kritériá pre prípadný návrat k pôvodnému stavu vrátane zaistenia konzistencie dát. Migračný postup musí obsahovať aj určenie zodpovedností, komunikačný režim počas zmeny a spôsob potvrdenia úspešného stabilizovania nového prostredia.

IV. Prevádzka a incident management

a) **Spracovanie chýb** - riešenie musí obsahovať jednotný mechanizmus zachytávania a spracovania chýb, ktorý zabraňuje úniku citlivých informácií. Každá chyba prezentovaná používateľovi musí obsahovať zrozumiteľnú správu a

jednoznačný identifikátor umožňujúci jej dohľadanie. Dodávateľ je povinný vytvoriť a priebežne udržiavať číselník chybových kódov dostupný 24/7, ktorý bude slúžiť ako referenčný zdroj pri nahlasovaní incidentov v rámci SLA. Logovanie chýb musí umožniť spätné dohľadanie technickej príčiny vrátane väzby na konkrétnu transakciu alebo integračný tok.

b) **Release proces** - nasadzovanie zmien musí prebiehať prostredníctvom jasne oddelených prostredí: vývojového, testovacieho a produkčného. Prechod medzi prostrediami musí byť kontrolovaný a auditovateľný. Buildy musia byť verzionované a archivované spôsobom umožňujúcim spätnú dohľadateľnosť a obnovu ľubovoľnej predchádzajúcej verzie. Pred nasadením do produkcie musí byť definovaný minimálny rozsah overenia zmien vrátane regresného testovania primeraného charakteru zmeny.

c) **Incident management -**dDodávateľ musí zabezpečiť nepretržitú podporu dostupnosti a funkcionality systému. Pri incidentoch súvisiacich s externými službami musí byť zabezpečené rozlíšenie incidentu podľa pôvodu a primeraná koordinácia s externým poskytovateľom. Incident management musí byť organizovaný v úrovniach s jasne definovanými reakčnými časmi a časmi zásahu pre každú úroveň závažnosti, doplnený o definované eskalačné pravidlá a pokrytie incidentov aj v období po nasadzovaní zmien alebo migráciách.

d) **RCA reporting** - pri závažných a kritických incidentoch dodávateľ vypracuje blameless analýzu o koreňovej príčine (RCA report) v štruktúre zahŕňajúcej popis incidentu, časový priebeh, identifikovanú príčinu, zhodnotenie dopadov, prijaté opatrenia a odporúčania na prevenciu opakovania. Správa musí byť dodaná do 72 hodín od vyriešenia incidentu, pri incidentoch s najvyššou závažnosťou do 24 hodín.

V. Spolupráca, handover a dokumentácia

a) **Pripravenosť na odovzdanie** Dodávateľ je povinný počas celej doby spolupráce udržiavať projekt v stave umožňujúcom jeho prevzatie obstarávateľom alebo iným dodávateľom bez neprimeraných nákladov alebo rizík. Dokumentácia architektúry, procesov a biznis logiky musí byť priebežne aktualizovaná a odovzdávaná, nie až na konci spolupráce. Súčasťou priebežnej dokumentácie musí byť aj evidencia kritických prevádzkových rozhodnutí a zmien architektúry prijatých počas spolupráce.

b) **Skúsenosti s citlivými systémami** verejný obstarávateľ identifikoval ako kľúčovú požiadavku skúsenosť s implementáciou alebo prevádzkou informačných systémov pracujúcich s citlivými údajmi alebo systémov závislých od externých

registrov, pričom **vyžaduje, aby takéto plnenia boli realizované v súlade s príslušnými bezpečnostnými štandardmi**. Z tohto dôvodu sa verejný obstarávateľ rozhodol zamerať na stanovenie požadovanej výslednej kvality plnenia, bez obmedzovania konkrétneho spôsobu jej dosiahnutia.

VI. Personálne zabezpečenie a kontinuita

a) **Personálne obsadenie tímu** Dodávateľ zabezpečí odborné kapacity. Ich kapacity musia zodpovedať rozsahu práce a musia byť primerane seniorné, aby bolo možné vykonávať všetky činnosti: prevzatie riešenia, audit, stabilizáciu, rozvoj, prevádzku, bezpečnosť aj riešenie incidentov.

- **Tech Lead / Architekt (0.5 – 1.0 FTE)** Zodpovedá za architektúru riešenia, technické štandardy, kontrolu kvality implementácie, riešenie komplexných technických incidentov (L3), návrhy refaktoringov a spoluprácu s MSP / HMBA pri technických rozhodnutiach. Je kľúčovým partnerom pri úvodnom prevzatí riešenia, analýze technického dlhu a návrhu stabilizačnej roadmapy.

- **Backend / Fullstack vývojár (min. 1 FTE)** Minimálne na úrovni medior, so skúsenosťami s NestJS, TypeScript, Prisma a PostgreSQL. Zodpovedajú za implementáciu backendových častí, integrácií na tretie strany (REST/SOAP), optimalizáciu výkonu a realizáciu úloh z backlogu. Musia byť schopní pracovať aj na úlohách súvisiacich s auditovanými a stabilizačnými krokmi.

- **Frontend / Fullstack vývojár (1 FTE)** So skúsenosťami minimálne na urovni medior s Next.js App Router. Zodpovedá za rozvoj používateľského rozhrania, implementáciu zmien vyplývajúcich z roadmapy, požiadaviek HMBA alebo auditov.

- **DevOps / Infra / SRE inžinier (0.5 – 1.0 FTE)** Zodpovedný za CI/CD pipeline, monitoring a alerting, nasadzovanie, správu prostredí, logovanie, správu kontajnerov, cloudových komponentov a podporu migračných a stabilizačných aktivít. Pri integráciách musí vedieť konfigurovať mechanizmy sledovania dostupnosti externých služieb a schopnosť identifikovať príčinu incidentu .

- **Projektový manažér / Delivery Manager / Scrum Master (0.3 – 0.5 FTE)** Riadi operatívne aktivity, koordinuje vývojový tím, plánuje sprinty, zabezpečuje komunikáciu s HMBA, riadi riziká a zodpovedá za reporting, vrátane výstupov z auditov, stabilizácie a incident managementu.

b) **Kontinuita a skúsenosti tímu** Rotácia členov tímu bez vážnych dôvodov je nežiaduca, a považuje sa za riziko pre zachovanie kontinuity prevádzky a rozvoja.

Dodávateľ musí zabezpečiť:

- stabilitu kľúčových členov tímu,
- plánované zmeny personálneho obsadenia len so súhlasom HMBA,
- náhradníkov s rovnakou alebo vyššou úrovňou kvalifikácie,
- dokumentáciu umožňujúcu prevzatie riešenia novým členom alebo HMBA bez neprimeraných nákladov,
- účasť vybraných odborníkov (minimálne projektový manažér, tech lead) na pravidelných osobných stretnutiach s business ownerom.
- Dodávateľ pri vyššie uvedených rolách garantuje osoby, ktoré majú: skúsenosť s projektami podobného rozsahu a charakteru,
- odbornú znalosť použitého technologického stacku (Next.js, NestJS, PostgreSQL/Prisma, Azure AD),
- schopnosť fungovať v tíme riadiacom sa agilnými princípmi,
- schopnosť komunikovať v slovenskom aj v anglickom jazyku.

Pri rolách projektového manažéra a tech leada/architekta sa očakáva schopnosť samostatne viesť odbornú diskusiu a formulovať technické odporúčania vo vzťahu k HMBA.

Konkrétne interné rozdelenie kapacít môže dodávateľ upraviť, ak preukáže schopnosť zabezpečiť všetky požadované činnosti v požadovanej kvalite a časových rámcoch.

Pri plnení predmetu zákazky sa očakáva pravidelná osobná pracovná súčinnosť dodávateľa so zástupcami HMBA, najmä pri úvodnom prevzatí riešenia, architektonických rozhodnutiach, prioritizácii backlogu a riešení kľúčových prevádzkových tém. Online forma spolupráce môže byť využívaná priebežne, avšak pri vybraných činnostiach sa predpokladá osobná účasť.

VII. Záväzky verejného obstarávateľa

a) **Jasne definovaný Business / Product Owner,** ktorý bude mať mandát rozhodovať o prioritách backlogu, kompetenciu akceptovať alebo neschvaľovať výstupy, možnosť rýchlo riešiť otázky týkajúce sa biznis logiky a právomoc robiť ad-hoc rozhodnutia počas nábehu a stabilizačnej fázy.

b) **Dostupnosť interných technických expertov počas úvodnej fázy –** verejný obstarávateľ zabezpečí dostupnosť interného experta, ktorý má znalosť aktuálneho riešenia a súčinnosť pri vysvetlení architektúry, procesu nasadzovania, biznisových tokov a histórie incidentov, knowledge transfer počas prvej fázy a možnosť konzultovať otázky súvisiace s predchádzajúcou

implementáciou. Ak interný tím nie je dostupný, bude možné akceptovať dlhšie trvanie technického auditu.

c) **Realistické očakávania počas úvodnej fázy –** verejný obstarávateľ akceptuje, že prevzatie riešenia **neznamená okamžitý rozvoj nových funkcionalít**, prvé 6–8 týždňov bude venovaných auditu, rekonštrukcii znalostí, stabilizácii a doplneniu dokumentácie, prvotné investície do stabilizácie sú nevyhnutné a nesmú byť považované za "práce navyše".

d) **Pripravený a prístupný backlog s jasnou prioritizáciou –** verejný obstarávateľ musí zabezpečiť existujúci zoznam známych incidentov, chýb a požiadaviek, priorizáciu backlogu zo strany Business Ownera, jednotné akceptačné kritériá a súčinnosť pri testovaní pre všetky úlohy, stabilitu požiadaviek v rámci sprintu, definované procesy pre schvaľovanie a zmeny priorít. Bez jasného backlogu nie je možné efektívne plánovať sprinty, rozvoj a stabilizáciu.