REPUBLIKA HRVATSKA
DRŽAVNA KOMISIJA ZA KONTROLU POSTUPAKA JAVNE NABAVE

KLASA: UP/II-034-02/25-01/587
URBROJ: 354-02/3-26-08
Zagreb, 26. svibnja 2026.

Državna komisija za kontrolu postupaka javne nabave, OIB: 95857869241, u Vijeću sastavljenom od članova: Maje Kuhar, predsjednice, Sanje Badrov Ranić, članice, i Gordana Klišanića, člana, u žalbenom postupku pokrenutom po žalbi žalitelja Rgo komunikacije d.o.o., Zagreb, OIB: 51551401153, na dokumentaciju o nabavi u otvorenom postupku javne nabave s namjerom sklapanja okvirnog sporazuma s jednim gospodarskim subjektom na razdoblje od 4 godine, broj objave: 2025/S F02-0011478, predmet nabave: održavanje RIS sustava, naručitelja Ministarstvo mora, prometa i infrastrukture, Zagreb, OIB: 22874515170, na temelju članka 3. Zakona o Državnoj komisiji za kontrolu postupaka javne nabave (Narodne novine, broj 18/13, 127/13, 74/14, 98/19 i 41/21) te članka 398. Zakona o javnoj nabavi (Narodne novine, broj 120/16, 114/22 i 48/26, dalje u tekstu: ZJN 2016) donosi sljedeće

R J E Š E N J E

1. Odbija se žalba žalitelja, Rgo komunikacije d.o.o., Zagreb, kao neosnovana.

2. Odbija se zahtjev za naknadom troška žalitelja, Rgo komunikacije d.o.o., Zagreb, kao neosnovan.

O b r a z l o ž e n j e

Naručitelj, Ministarstvo mora, prometa i infrastrukture, Zagreb, objavio je 6. listopada 2025. u Elektroničkom oglasniku javne nabave Republike Hrvatske (dalje u tekstu: EOJN RH) poziv na nadmetanje s dokumentacijom o nabavi u otvorenom postupku javne nabave s namjerom sklapanja okvirnog sporazuma s jednim gospodarskim subjektom na razdoblje od 4 godine, broj objave: 2025/S F02-0011478, predmet nabave: održavanje RIS sustava. Kriterij odabira je ekonomski najpovoljnija ponuda, koja se određuje na temelju cijene i kvalitete - specifično iskustvo stručnjaka za sigurnost informacijskih sustava br. 1 (S1) i specifično iskustvo stručnjaka za sigurnost informacijskih sustava br. 2 (S2).

Na dokumentaciju o nabavi urednu žalbu je 15. listopada 2025. izjavio žalitelj Rgo komunikacije d.o.o., Zagreb.

Žalitelj u žalbi, u bitnome, osporava zakonitost dijela dokumentacije o nabavi te predlaže poništenje dijelova dokumentacije o nabavi za koje smatra da su nezakoniti. Ujedno zahtijeva naknadu troškova žalbenog postupka u iznosu od 3.120,00 eura.

Naručitelj u odgovoru predlaže odbiti žalbu žalitelja kao neosnovanu.

U tijeku postupka pred ovim tijelom izvedeni su dokazi pregledom i analizom dokaznog materijala koji se sastoji od obavijesti o nadmetanju, dokumentacije o nabavi te ostalih dokaza.

Žalba je dopuštena, pravodobna i uredna te izjavljena od ovlaštene osobe.

Žalba je neosnovana.

Žalitelj u žalbi navodi da je naručitelj u dokumentaciji o nabavi, pod točkom 5.2 Tehnička i stručna sposobnost, odredio uvjet 5.2.2. Tehnički stručnjaci ili tijela – kontrola kvalitete, pri čemu je broj stručnjaka i uvjete za njih definirao u točki 5.2.2.4., a koji uvjeti nisu propisani u skladu s člankom 256. stavcima 3. i 4. ZJN 2016. Navedeno temelji na analizi dokumentacije i RIS sustava danoj u Prilogu 1 uz žalbu te na stručnom poznavanju karakteristika hrvatskog RIS sustava, budući da je izvršavao uslugu njegova održavanja u razdoblju od 2000. do lipnja 2024. godine. Navodi da su tehničke specifikacije i karakteristike RIS sustava identične onima iz prethodnog ugovora o održavanju, radi čega smatra da ima odgovarajući stručni uvid za ocjenu povezanosti i razmjernosti traženih uvjeta sposobnosti s predmetom nabave.

Žalitelj smatra da uvjeti propisani za stručnjake S1, S2, S3, S5 i S6 nisu povezani s predmetom nabave niti su mu razmjerni. Osobito ističe stručnjake S1 i S2, navodeći da su tražena čak dva stručnjaka za informacijsku sigurnost, uz velik broj uvjeta vezanih uz njihovo iskustvo i djelomično preklapanje traženih uvjeta, iako tehničke specifikacije, ne upućuju na aktivnosti vezane uz sigurnost informacijskih sustava tijekom izvršenja ugovora.

Nadalje, žalitelj smatra da uvjet prema kojem ponuditelj mora osigurati osam stručnjaka, pri čemu ista osoba ne može obavljati više stručnih pozicija, nije razmjeran predmetu nabave s obzirom na procijenjenu vrijednost i opis usluge.

Žalitelj u Prilogu 1, dostavljenom uz žalbu, iznosi detaljno obrazloženje žalbenih navoda kako slijedi.

U odnosu na stručnjaka S1 ističe da tehničke specifikacije ne predviđaju WAF rješenje i multi faktorsku autentifikaciju kao dio RIS sustava niti su ta rješenja implementirana kao njegove funkcionalnosti, dok za DoS i DDoS zaštitu, sustav za nadzor i zaštitu baze podataka te održavanje IT sigurnosnih sustava navodi da tehničke specifikacije ne predviđaju aktivnosti vezane uz takve usluge. Nadalje, u odnosu na WAF rješenje i sustav za nadzor i zaštitu baze podataka posebno ističe da se predmet nabave odnosi na održavanje postojećeg RIS sustava, a ne na njegovu nadogradnju ili implementaciju novih sigurnosnih rješenja. Nadalje navodi da je za iskustvo vezano uz implementaciju WAF rješenja, DoS i DDoS zaštite te sustava za nadzor i zaštitu baze podataka propisan uvjet iskustva na softverima za minimalno 1000 dnevnih korisnika, dok je za iskustvo na projektu implementacije sustava za multi faktorsku autentifikaciju propisan uvjet iskustva na softverima za minimalno 200 dnevnih korisnika. Smatra da su navedeni pragovi nerazmjerni predmetu nabave budući da je RIS sustav u razdoblju 2020. – 2024. imao ukupno 74 registrirana korisnika, dok se dnevno na sustav spajalo do 10 korisnika.

U odnosu na stručnjaka S2 ističe da tehničke specifikacije ne predviđaju aktivnosti implementacije sustava informacijske sigurnosti, strategije informacijske sigurnosti, upravljanja sigurnosnim incidentima i procjene rizika, kao ni implementaciju zaštite baze podataka i SOAR rješenja kao dijela RIS sustava niti je SOAR rješenje implementirano kao funkcionalnost postojećeg sustava. Kod iskustva sudjelovanja kao voditelja tima za sigurnost informacijskih sustava ističe da tehničke specifikacije ne predviđaju uspostavu i vođenje tima pri čemu ističe da u okviru projekta nije predviđen nikakav tim posebice onaj vezan za sigurnost informacijskog sustava.

Nadalje navodi da je za iskustvo vezano uz implementaciju zaštite baze podataka propisan uvjet koji je sadržajno gotovo identičan četvrtom uvjetu propisanom za stručnjaka S1, čime se dodatno naglašava nerazmjernost uvjeta.

U odnosu na stručnjaka S3 žalitelj navodi da tehničke specifikacije ne predviđaju korištenje tehnologija navedenih u zahtjevu da stručnjak mora imati iskustvo u minimalno jednom završenom projektu dizajniranja IT sustava primjenom DevOps praksi uz korištenje alata CI/CD pipelines, Jenkins, Docker, Kubernetes i OpenShift Container Platform u svojstvu stručnjaka za arhitekturu, niti su iste implementirane u RIS sustav. Ističe da tehničke specifikacije ne sadržavaju aktivnosti vezane uz dizajniranje IT sustava niti uz primjenu navedenih tehnologija, dok se predmet nabave odnosi na održavanje, a ne na nadogradnju sustava koja bi uključivala izgradnju arhitekture sustava. Dodatno smatra da je uvjet nerazmjeran jer se traži iskustvo u korištenju svih navedenih tehnologija i alata. Nadalje, u odnosu na zahtjev da stručnjak mora imati iskustvo na najmanje jednom završenom projektu dizajniranja skalabilnih, modularnih i sigurnih sustava u svojstvu stručnjaka za arhitekturu, žalitelj navodi da tehničke specifikacije ne sadržavaju aktivnosti vezane uz dizajniranje takvog sustava.

U odnosu na stručnjaka S5 žalitelj navodi da tehničke specifikacije ne predviđaju korištenje tehnologija navedenih u zahtjevu da stručnjak mora imati iskustvo u minimalno jednom završenom projektu izrade baze podataka primjenom tehnologija Oracle, PostgreSQL, MySQL, PL/SQL, Docker, GitLab CI/CD, Ansible, Prometheus, Grafana i AWS u svojstvu stručnjaka za baze podataka, niti su iste implementirane u RIS sustav, pri čemu ističe da se u sklopu RIS sustava koristi isključivo PostgreSQL. Nadalje ističe da tehničke specifikacije ne sadržavaju aktivnosti vezane uz izradu baze podataka uz primjenu svih navedenih tehnologija, pri čemu se dodatno naglašava nerazmjernost uvjeta budući da se traži iskustvo u korištenju svih navedenih tehnologija, iako se iste međusobno isključuju, osobito u dijelu baza podataka gdje je moguće koristiti samo jednu tehnologiju (Oracle, PostgreSQL ili MySQL). Jednake prigovore žalitelj iznosi u odnosu na minimalno iskustvo za stručnjaka S6 kojim se traži iskustvo u minimalno jednom završenom projektu izrade ili održavanja IT sustava primjenom tehnologija Oracle, PostgreSQL, MySQL, PL/SQL, Docker, GitLab CI/CD, Ansible, Prometheus, Grafana i AWS u svojstvu stručnjaka za sistem administraciju.

Žalitelj ujedno dostavlja dokument Prilog II u kojem se u bitnome navode podaci o prethodno provedenom postupku javne nabave objavljenom pod brojem 2019/S 0F2-0051311 te obavijesti o sklopljenom ugovoru objavljenoj pod brojem 2020/S 002-001894. Žalitelj ističe da uvid u tehničke specifikacije iz navedenog postupka ukazuje na gotovo istovjetan opis usluga kao i u postupku nabave koji je predmet ovog žalbenog postupka. Nadalje navodi da su u ranijem postupku bili propisani znatno uži uvjeti tehničke i stručne sposobnosti u odnosu na tražene stručnjake, pri čemu je bilo predviđeno raspolaganje s tri profila stručnjaka i najmanje po tri stručnjaka za svaki profil, uz mogućnost da ista osoba obavlja više funkcija.

Naručitelj u odgovoru na žalbu navodi da je dokumentacijom o nabavi propisao minimalne uvjete tehničke i stručne sposobnosti potrebne za održavanje i zaštitu svojeg integriranog informacijskog sustava, čiji je sastavni dio i hrvatski RIS sustav. Ističe da su traženi stručnjaci S1–S8 izravno povezani s poslovima održavanja navedenog sustava te da su, slijedom toga, zahtijevani stručni profili opravdani.

Nadalje, naručitelj se poziva na obveze koje za njega proizlaze iz Zakona o kibernetičkoj sigurnosti, ističući da navedeni zakon nije bio na snazi u vrijeme sklapanja ranijih ugovora na koje se žalitelj poziva. Navodi da je u ožujku 2025. godine, temeljem navedenog zakona, kategoriziran kao ključni subjekt s utvrđenom visokom razinom kibernetičkih rizika te da je stoga obvezan osigurati visoku razinu zaštite svojeg informacijskog i komunikacijskog sustava. U prilog navedenome dostavlja dopis Ureda Vijeća za nacionalnu sigurnost od 20. ožujka 2025. godine. S tim u vezi, naručitelj obrazlaže potrebu angažiranja stručnjaka (S1 i S2) zbog rizika od DoS/DDoS napada, zaštite baza podataka, multifaktorske autentifikacije i drugih sigurnosnih prijetnji, zatim stručnjaka za sistemsku administraciju i DevOps (S6) radi osiguranja kontinuirane isporuke i integracije (CI/CD), monitoring i brzog reagiranja na incidente, te stručnjaka za arhitekturu sustava (S3) radi osiguravanja skalabilnosti, sigurnosti i dugoročne održivosti sustava. U odnosu na načelo

razmjernosti, naručitelj smatra da su propisani uvjeti opravdani složenošću integriranog sustava i usklađeni s tehničkim specifikacijma. Ističe da osam stručnjaka ne predstavlja nerazmjeran zahtjev s obzirom na to da sustav obuhvaća cijelu mrežu hrvatskih vodnih putova, ima međunarodnu povezanost i korisnike, zahtijeva neprekidnu dostupnost te visoku razinu zaštite od sve učestalijih i sofisticiranijih kibernetičkih prijetnji, te ispunjava uvjete povezivanja s europskim RIS sustavom koji obuhvaća 27.000 km plovnih putova.

Naručitelj navodi da žalitelj pogrešno smatra da WAF nije dio RIS sustava jer nije posebno naveden u tehničkim specifikacijama, no naručitelj ističe da specifikacije ne moraju sadržavati sve sigurnosne i infrastrukturne komponente, posebno kod složenih i kritičnih sustava. Ističe da se RIS sustav sastoji od web aplikacija, API servisa i integracijskih točaka koje su izložene mrežnim prijetnjama, a WAF je sigurnosni sloj ispred aplikacija koji se u pravilu ne opisuje kroz poslovne funkcionalnosti nego kroz sigurnosnu arhitekturu, pa njegovo nenavođenje ne znači da nije relevantan za održavanje. Naručitelj dalje navodi da žalitelj pogrešno shvaća održavanje kao isključivo tehničke ispravke i administraciju, dok ono kod sustava nacionalne važnosti uključuje stalno prilagođavanje sigurnosnih pravila, reakcije na napade (OWASP Top 10, zero-day), analizu logova i usklađivanje s propisima (npr. Zakon o kibernetičkoj sigurnosti, NIS2 i EU RIS inicijative). Zato se WAF iskustvo traži radi sposobnosti održavanja i nadzora sigurnosnog sloja, a ne radi nove implementacije, jer ono zahtijeva široko tehničko razumijevanje aplikacija, protokola i sigurnosnih mehanizama. Također se odbacuje usporedba broja registriranih korisnika s kriterijem „1000 dnevnih korisnika“, jer se to ne odnosi na veličinu sustava nego na razinu izloženosti, rizika i opterećenja u produkciji. Taj kriterij se koristi kao pokazatelj složenosti sigurnosnih izazova, a ne kao statistička usporedba korisnika. Sustavi s većom izloženošću imaju veće sigurnosne zahtjeve, više napada i strože SLA uvjete, pa iskustvo u takvim okruženjima znači veću razinu stručnosti primjenjivu i na RIS sustav. Naručitelj dodatno navodi da pojam „dnevni korisnici“ predstavlja standardni stručni kriterij u IT praksi za mjerenje opterećenja, rizika i skalabilnosti sustava te se koristi u procjeni iskustva i sigurnosne složenosti, a može se dokazivati kroz tehničku dokumentaciju, SLA-ove i izvješća o korištenju. Na kraju se ističe da je RIS sustav integriran u zajedničku mrežu s više od 25.000 korisnika i da zbog njegovog sistemskog značaja i potencijalnih posljedica incidenata naručitelj ima pravo tražiti višu razinu stručnosti.

Naručitelj zaključuje se da su uvjeti povezani s predmetom nabave, razmjerni rizicima, da ne moraju odgovarati prethodnom stanju sustava te da naručitelj ima pravo predvidjeti buduće sigurnosne potrebe. Također se smatra da je dokumentacija jasna i da eventualna nejasnoća proizlazi iz stajališta žalitelja, a ne iz samog teksta.

Naručitelj nadalje navodi da se navodi žalitelja temelje se na pogrešnoj i pojednostavljenoj pretpostavci da se karakteristike RIS sustava mogu sagledavati isključivo kroz popis funkcionalnosti iz tehničkih specifikacija, bez uzimanja u obzir arhitekture sustava, sigurnosnog modela, operativnog okruženja i regulatornih obveza. Naručitelj ističe da RIS sustav nije izolirana aplikacija s ograničenim brojem korisnika, već dio integriranog informacijskog sustava Ministarstva mora, prometa i infrastrukture, povezan s nacionalnim i međunarodnim sustavima te izložen javnim i polujavnim mrežama, uz obvezu osiguravanja dostupnosti, integriteta i povjerljivosti podataka.

Ističe da se stvarne karakteristike sustava ne određuju se samo brojem korisnika iz nekog razdoblja, nego razinom izloženosti prijetnjama, važnošću podataka, zahtjevima 24/7 dostupnosti te ulogom sustava u sigurnosti plovidbe i međunarodnoj razmjeni podataka. U odnosu na WAF, naručitelj navodi da je riječ o horizontalnom sigurnosnom sloju u arhitekturi informacijskog sustava koji je smješten između mrežnog i aplikacijskog sloja koji štiti od napada poput SQL injection, XSS, CSRF, bot napada te DoS/DDoS napada.

Takva zaštita smatra se nužnim dijelom održavanja RIS sustava, iako nije poslovna funkcionalnost sustava. Naručitelj navodi da je održavanje RIS sustava uključuje kontinuirano praćenje sigurnosnih događaja, prilagodbu sigurnosnih pravila novim obrascima napada, analizu

logova i suradnju sigurnosnih slojeva sustava. Zbog toga je iskustvo u implementaciji WAF rješenja traženo jer omogućuje razumijevanje interakcije sigurnosnog sloja i aplikacijske arhitekture, razlikovanje legitimnog i zlonamjernog prometa te sprječavanje incidenata bez narušavanja dostupnosti sustava. U pogledu ZJN 2016, naručitelj smatra da je uvjet povezan s predmetom nabave jer se odnosi na sigurnost i dostupnost sustava te razmjernost procjenjuje kroz rizike sustava, a ne kroz statistiku korištenja. Ističe se da uvjeti sposobnosti ne moraju biti ograničeni na postojeće stanje sustava, nego moraju osigurati kvalitetno i sigurno izvršenje ugovora te uzeti u obzir rast sigurnosnih prijetnji i regulatorne zahtjeve (kibernetička sigurnost, NIS2, EU RIS). Također se navodi da sigurnosne aktivnosti, uključujući WAF i zaštitu od DoS/DDoS napada, čine sastavni dio održavanja informacijskih sustava od nacionalne važnosti, neovisno o tome koliko su detaljno opisane u tehničkim specifikacijama. Naručitelj smatra da je dokumentacija jasna i precizna jer jasno definira traženo iskustvo i prag dnevnih korisnika te omogućuje razumijevanje zahtjeva i izradu ponude.

Naručitelj smatra da žalitelj pogrešno i nepotpuno tumači RIS sustav jer ga promatra samo kroz vidljive funkcionalnosti i broj korisnika, bez uzimanja u obzir arhitekture, sigurnosnog modela, operativnog okruženja i regulatornih obveza. Ističe da je RIS sustav centralizirani sustav od posebnog značaja za sigurnost plovidbe i međunarodnu razmjenu podataka, koji obrađuje osjetljive podatke, integriran je s nacionalnim i međunarodnim sustavima te mora osigurati visoku razinu dostupnosti, pouzdanosti i sigurnosti neovisno o broju korisnika.

Stvarne karakteristike sustava, prema naručitelju, proizlaze iz razine sigurnosnog rizika, potrebe zaštite pristupa, sljedivosti i usklađenosti s nacionalnim i EU propisima. U odnosu na MFA, naručitelj navodi da je riječ o temeljnom sigurnosnom mehanizmu IAM sustava koji se može implementirati na različitim razinama (aplikacija, IdP, infrastruktura). Održavanje RIS sustava uključuje upravljanje identitetima i pristupom, zaštitu od kompromitacije računa, phishinga i neovlaštenog pristupa, pa je iskustvo u implementaciji MFA rješenja relevantno za razumijevanje i održavanje tih sigurnosnih mehanizama. U tom kontekstu održavanje RIS sustava podrazumijeva upravljanje korisničkim identitetima i pravima pristupa, osiguravanje pouzdane autentifikacije korisnika, zaštitu od kompromitacije korisničkih računa, smanjenje rizika od krađe identiteta, phishing napada i neovlaštenog pristupa. Iskustvo stručnjaka u implementaciji MFA rješenja nužno je kako bi se osiguralo razumijevanje različitih MFA modela (TOTP, OTP, push notifikacije, certifikati, FIDO2, smart kartice), integracije MFA mehanizama s postojećim aplikacijama i servisima te održavanja i prilagodbe autentifikacijskih politika tijekom trajanja ugovora. Ističe se da MFA zahtijeva znanje različitih metoda autentifikacije (TOTP, OTP, push, certifikati, FIDO2, smart kartice) te njihovu integraciju i održavanje kroz životni vijek sustava. Naručitelj dodatno navodi da žalitelj pogrešno shvaća održavanje kao zadržavanje postojećeg stanja, dok ono u praksi uključuje stalnu sigurnosnu prilagodbu, uvođenje novih sigurnosnih mehanizama i usklađivanje s novim prijetnjama i regulativom. Zato je opravdano tražiti iskustvo u MFA implementacijama i radu na sustavima s većim brojem korisnika zbog pitanja skalabilnosti, dostupnosti i sigurnosti. U smislu ZJN 2016, uvjet se smatra povezan s predmetom nabave jer se odnosi na sigurnost, pouzdanost i kontrolu pristupa RIS sustavu te je razmjeran njegovoj složenosti i rizicima, a ne samo broju korisnika. Naručitelj ima obvezu osigurati stručnog izvršitelja i smanjiti rizike sigurnosnih incidenata. Također se navodi da MFA predstavlja horizontalni sigurnosni sloj koji nije uvijek eksplicitno naveden u tehničkim specifikacijama, a održavanje sustava obuhvaća i održavanje sigurnosnog modela.

Žalitelj u podnesku od 22. listopada 2025. navodi da se naručitelj u odgovoru na žalbu očitovao samo djelomično, odnosno isključivo u odnosu na dio navoda koji se odnosi na stručnjake S1, S2, S3 i S6, dok se uopće nije očitovao na žalbene navode koji se odnose na stručnjaka S5. U odnosu na pozivanje naručitelja na Zakon o kibernetičkoj sigurnosti i dopis Ureda Vijeća za nacionalnu sigurnost, žalitelj navodi da iz tog dopisa proizlazi isključivo da je naručitelj kategoriziran kao ključni subjekt, ali se u njemu ne navodi RIS sustav niti bilo kakve posebne obveze koje bi se

odnosile na predmet nabave. Ističe da predmet nabave nije održavanje integriranog informacijskog sustava naručitelja, nego isključivo RIS sustava, te ističe da dokumentacija o nabavi nigdje ne potvrđuje da bi RIS sustav bio dio integriranog informacijskog sustava naručitelja. Smatra da bi, da je RIS sustav doista dio takvog integriranog sustava, tehnička specifikacija morala sadržavati informacije o cjelokupnom integriranom sustavu naručitelja. Nadalje, žalitelj ističe da se eventualne obveze koje proizlaze iz propisa o kibernetičkoj sigurnosti moraju jasno i nedvojbeno navesti u dokumentaciji o nabavi, osobito u opisu predmeta nabave i tehničkim specifikacijama. Dalje navodi da se u dokumentaciji o nabavi ne navode nikakve odredbe niti su opisane aktivnosti ugovaratelja, odnosno stručnjaka, u vezi sa zaštitom informacijskog i komunikacijskog sustava. Žalitelj ističe da naručitelj u odgovoru na žalbu samo općenito navodi razloge uključivanja stručnjaka S1, S2, S3 i S6. S tim u vezi ističe da se u postupku javne nabave ne mogu „podrazumijevati“ obveze ili aktivnosti koje nisu izričito i jasno propisane dokumentacijom o nabavi. Time, prema mišljenju žalitelja, naručitelj zapravo potvrđuje da traženi uvjeti za stručnjake u dijelu koji se odnosi na informacijsku sigurnost nisu utemeljeni na predmetu nabave niti jasno proizlaze iz dokumentacije o nabavi. Također ističe da se naručitelj uopće nije očitovao na većinu konkretnih prigovora iz Priloga 1 žalbe, uključujući uvjete koji se odnose na broj korisnika sustava, tražene tehnologije i alate (npr. WAF, SOAR, Oracle, MySQL), razvoj i implementaciju strategije informacije sigurnosti, vođenja tima itd…

Zaključno, žalitelj navodi da se naručitelj u pogledu razmjernosti ograničio na općenite tvrdnje o složenosti sustava, pri čemu se ponovno poziva na elemente koji nisu sadržani u dokumentaciji o nabavi. Posebno ističe da je pozivanje na povezanost RIS sustava s europskim RIS sustavom i 27.000 km plovnih putova neosnovano i nerelevantno, budući da se predmet nabave odnosi isključivo na nacionalni RIS sustav, bez ikakve reference na širi europski sustav u dokumentaciji o nabavi.

Naručitelj u podnesku od 28. siječnja 2026. u bitnome navodi da prilikom sastavljanja odgovora na žalbu nije smatrao potrebnim pojedinačno se očitovati na svaki navod iz Priloga I žalbe jer smatra da je iz ranijeg odgovora razvidno da se isti odnosi na sve tražene stručnjake. U tom smislu navodi da je uvjete tehničke i stručne sposobnosti obrazložio kroz funkcionalne cjeline integriranog RIS sustava, a ne parcijalno po pojedinim stručnjacima. Slijedom navedenog osporava tvrdnju žalitelja da se nije očitovao na stručnjaka S5 te navodi da stručnjak za baze podataka i aplikacijsku infrastrukturu proizlazi iz zahtjeva vezanih uz zaštitu podataka, dostupnost sustava i kontinuitet rada. Nadalje navodi da je pogrešan žaliteljev navod prema kojem RIS sustav nije dio integriranog informacijskog sustava naručitelja. Ističe da RIS sustav predstavlja sastavni dio njegovog informacijskog sustava s obzirom na vlasništvo i upravljanje sustavom, njegovu povezanost s drugim državnim i međunarodnim informacijskim sustavima te zakonske obveze koje se odnose na cjelokupni IKT okoliš ključnog subjekta.

U odnosu na navod žalitelja da bi dokumentacija o nabavi trebala sadržavati informacije o cjelokupnom integriranom informacijskom sustavu, naručitelj navodi da ne postoji obveza izlaganja kompletne interne arhitekture sustava te da načelo razmjernosti i sigurnosti opravdava ograničavanje objave osjetljivih tehničkih podataka, osobito kod sustava koji predstavljaju dio kritične infrastrukture dok su uvjeti sposobnosti povezani s realnim okruženjem u kojem se taj sustav nalazi.

Naručitelj nadalje navodi da žalitelj pogrešno tumači primjenu Zakona o kibernetičkoj sigurnosti smatrajući da se njegove odredbe primjenjuju isključivo u slučaju kada je pojedini podsustav izrijekom naveden u aktu kategorizacije. Ističe da takvo tumačenje nije u skladu s normativnom logikom Zakona, prema kojem se kategorizacija odnosi na subjekt kao cjelinu, a ne na pojedinačne aplikacije, dok se obveze zaštite odnose na sve informacijske i komunikacijske sustave kojima se subjekt koristi u obavljanju svojih ključnih funkcija. U tom smislu navodi da RIS sustav, kao sustav koji obrađuje podatke od značaja za sigurnost plovidbe, ima stalnu dostupnost te je povezan s međunarodnim sustavima, nesporno ulazi u opseg primjene sigurnosnih mjera,

neovisno o tome je li izrijekom naveden u dopisu Ureda Vijeća za nacionalnu sigurnost. Naručitelj također osporava navode žalitelja da dokumentacija o nabavi ne predviđa aktivnosti vezane uz informacijsku i kibernetičku sigurnost. U tom smislu upućuje na tehničku specifikaciju kojom je predviđena izmjena aplikacijskih i operativnih sustava, kao i na članak 16. Prijedloga okvirnog sporazuma kojim su propisane obveze izvršitelja da postupa u skladu s važećim mjerama i standardima informacijske sigurnosti te pravilima postupanja s klasificiranim i neklasificiranim podacima koji su mu dostupni tijekom izvršenja ugovora. Navedene obveze odnose se, između ostaloga, na podatke povezane s komunikacijskom opremom i terminalnim uređajima, financijskim podacima, podacima o postupcima nabave te drugim podacima čije bi neovlašteno ili nepravilno korištenje, umnožavanje ili otkrivanje moglo prouzročiti materijalnu ili nematerijalnu štetu te ugroziti sigurnost, interese i poslovanje naručitelja. Istim člankom izvršitelj se obvezuje postupati sukladno odredbama Zakona o informacijskoj sigurnosti (NN 79/07, 14/24), Zakona o tajnosti podataka (NN 79/07, 86/12) te Zakona o kibernetičkoj sigurnosti, kao i internim aktima naručitelja iz područja informacijske sigurnosti. S tim u vezi ukazuje da žalitelj nije osporavao odredbe dokumentacije koje se odnose na primjenu pravila primjenu pravila informacijske i kibernetičke sigurnosti niti je tražio pojašnjenje dokumentacije u tom smislu.

Nadalje se u očitovanju poziva na odredbe članka 12. i članka 25. Zakona o kibernetičkoj sigurnosti te ističe da je naručitelj središnje tijelo državne uprave i očekuje da je ta činjenici poznata zainteresiranim gospodarskim subjektima. U tom smislu poziva se i na Izvješće Agencije Europske unije za kibersigurnost o stanju prijetnji za 2025. godinu prema kojem su javna uprava i promet među najpogođenijim sektorima po broju kibernetičkih incidenata. Naručitelj ističe da žaliteljev prigovor kako se sigurnosne aktivnosti ne navode u tehničkim specifikacijama proizlazi iz pogrešnog i formalističkog tumačenja odnosa između tehničkih specifikacija i uvjeta tehničke i stručne sposobnosti. S tim u vezi ističe da tehničke specifikacije opisuju što se održava, dok se uvjeti tehničke i stručne sposobnosti odnose na potrebna znanja i iskustvo izvršitelja za njezino zakonito i stručno izvršenje. Slijedom navedenog, naručitelj smatra da u tehničkim specifikacijama nije potrebno taksativno navoditi svaku pojedinu sigurnosnu aktivnost.

U odnosu na žalbene navode o nerazmjernosti i „nepovezanim tehnologijama“ poput WAF-a, SOAR-a, Oraclea i MySQL-a, naručitelj navodi da RIS sustav nije izolirana aplikacija već produkcijski sustav visoke dostupnosti koji koristi standardne enterprise tehnologije i koji mora biti zaštićen sukladno suvremenim sigurnosnim standardima. Smatra da traženi uvjeti predstavljaju minimalni skup znanja potreban za održavanje sustava takve vrste i razine rizika. Nadalje navodi da se razmjernost uvjeta procjenjuje u odnosu na opseg sustava, teritorijalnu pokrivenost i međunarodnu interoperabilnost sustava, dok pozivanje na europski RIS sustav ne predstavlja proširenje predmeta nabave već argument u prilog složenosti i interoperabilnosti nacionalnog RIS sustava.

Naručitelj je uz podnesak dostavio i očitovanje na Prilog I, u kojem se očituje o navodima žalitelja koji se odnose na stručnjake S1, S2, S3, S5 i S6. Naručitelj u bitnom navodi se žaliteljeve tvrdnje temelje na preuskom tumačenju tehničkih specifikacija te ističe da održavanje RIS sustava, kao sustava od javnog interesa, obuhvaća sigurnosne, operativne i tehničke aspekte nužne za njegovo sigurno, stabilno i kontinuirano funkcioniranje. U tom kontekstu, traženi uvjeti iskustva odnose se na aktivnosti koje naručitelj smatra relevantnima za kvalitetno i sigurno održavanje RIS sustava, iako te aktivnosti nisu formalno navedene u tehničkim specifikacijama.

Naručitelj nadalje ističe da se osporeni uvjeti iskustva ne odnose na proširenje predmeta nabave niti na uvođenje novih usluga, već isključivo na prethodno iskustvo stručnjaka, koje služi kao pokazatelj njihove sposobnosti za kvalitetno i sigurno izvršenje ugovornih obveza. U pogledu usklađenosti s odredbama ZJN 2016, naručitelj smatra da su predmetni uvjeti izravno povezani s predmetom nabave te razmjerni njegovoj složenosti i rizicima sukladno članku 256. stavku 3. ZJN 2016. Nadalje, naručitelj ističe da se zahtjevi vezani uz sigurnost informacijskog sustava povezuju i s obvezama iz područja kibernetičke sigurnosti, budući da je cilj osigurati zaštitu integriteta,

povjerljivosti i dostupnosti podataka te otpornost sustava na sigurnosne prijetnje i incidente u skladu s relevantnim propisima iz područja kibernetičke sigurnosti.

Ocjenjujući žalbene navode utvrđeno je sljedeće činjenično stanje.

U tijeku žalbenog postupka izvršen je uvid u točku 3.1. Opis predmeta nabave utvrđeno je da se u istoj navodi da je predmet nabave održavanje RIS sustava sukladno troškovniku, tehničkoj specifikaciji i ostalim traženim uvjetima naznačenima u ovoj Dokumentaciji o nabavi. Uvidom u troškovnik utvrđeno je da se traži nuđenje cijene za održavanje RIS sustava gdje se su ponuditelju u rekapitulaciji bili dužni ponuditi cijenu po stavkama: trošak preventivnog održavanja, korektivnog održavanja – popravak, korektivnog održavanja – zamjena. Uvidom u tehničku specifikaciju utvrđeno je da se u istoj između ostalog navodi: „ predmet nabave su usluge preventivnog i korektivnog održavanja RIS sustava.“ „Hrvatski RIS sustav zahtijeva korektivno i preventivno održavanje na pet razina: 1. Uređaji i oprema, 2. AIS informacijski sustav (BSC - kontroleri baznih stanica, LSS - serverske AIS aplikacije, AIS web aplikacije, ECDIS web aplikacije, ECDIS preglednici, Nagios sustav za nadzor i detekciju kvarova), 3. VHF komunikacijski sustav, 4. RIS aplikacijski sustav (RIS preglednik – Korisnička aplikacija, Web Baza podataka o trupu plovila, RIS index, Web NTS aplikacija - priopćenja brodarima, Bottleneck web service, Fairway Availability web service, Web LSS HR/SAVA – Upravljanje RIS infrastrukturom i korisničkim pristupom) i 5. Podrška korisnicima za RIS aplikacijski sustav.“

Uvidom u Kriterij za kvalitativni odabir gospodarskog subjekta s uputama – točka 5.2.2 tehnički stručnjaci i tijela – kontrola kvalitete, točka 5.2.2.3 Dodatno pojašnjenje kriterija propisano je: “ Naručitelj je odredio minimalne uvjete tehničke i stručne sposobnosti sukladno odredbama ZJN 2016. Naime, s obzirom na predmet nabave i rokove izvršenja predmetnih usluga, naručitelj je propisao da izvršitelj mora raspolagati s minimalno 8 (osam) traženih stručnjaka kako bi bio u mogućnosti uspješno izvršiti predmetne usluge.“…“ Zbog opsega posla i geografske rasprostranjenosti cjelokupnog sustava, isti stručnjaci ne mogu ispunjavati uvjete iz svih osam točaka, odnosno Naručitelj ne dozvoljava da ista osoba zauzme više pozicija stručnjaka.“ Pod točkom 5.2.2.4 Uvjeti propisano je: „ Tehnički stručnjak S1 - Stručnjak za sigurnost informacijskih sustava br. 1 - najmanje 1 (jedan) stručnjak. Stručnjak mora imati iskustvo u: minimalno jednom završenom projektu implementacije WAF rješenja za zaštitu web aplikacija u svojstvu stručnjaka za sigurnost informacijskih sustava na softverima za minimalno 1000 dnevnih korisnika; minimalno jednom završenom projektu implementacije DoS i DDoS rješenja u svojstvu stručnjaka za sigurnost informacijskih sustava na softverima za minimalno 1000 dnevnih korisnika; minimalno jednom završenom projektu implementacije sustava za multi faktorsku autentifikaciju u svojstvu stručnjaka za sigurnost informacijskih sustava na softverima za minimalno 200 dnevnih korisnika; minimalno jednom završenom projektu implementacije sustava za nadzor i zaštitu baze podataka u svojstvu stručnjaka za sigurnost informacijskih sustava na softverima za minimalno 1000 dnevnih korisnika; minimalno jednom završenom projektu održavanja IT sigurnosnih sustava u svojstvu stručnjaka za sigurnost informacijskih sustava. Tehnički stručnjak S2 - Stručnjak za sigurnost informacijskih sustava br. 2 - najmanje 1 (jedan) stručnjak. Stručnjak mora imati iskustvo u: minimalno jednom završenom projektu iz područja implementacije sustava informacijske sigurnosti u kojem je stručnjak sudjelovao u svojstvu stručnjaka za sigurnost informacijskih sustava; minimalno jednom završenom projektu razvoja i implementacije strategije informacijske sigurnosti u kojem je stručnjak sudjelovao u svojstvu stručnjaka za sigurnost informacijskih sustava; minimalno jednom završenom projektu u kojem je stručnjak sudjelovao u svojstvu voditelja tima za sigurnost informacijskih sustava; minimalno jednom završenom projektu upravljanja sigurnosnim incidentima i procjenom rizika u kojem je stručnjak sudjelovao u svojstvu stručnjaka za sigurnost informacijskih sustava; minimalno jednom završenom projektu implementacije zaštite baze podataka u kojem je stručnjak sudjelovao u svojstvu stručnjaka za

sigurnost informacijskih sustava; minimalno jednom završenom projektu implementacije SOAR rješenja u kojem je stručnjak sudjelovao u svojstvu stručnjaka za sigurnost informacijskih sustava. Tehnički stručnjak S3 - Stručnjak za arhitekturu informacijskih sustava - najmanje 1 (jedan) stručnjak. Stručnjak mora imati iskustvo u: minimalno jednom završenom projektu dizajniranja IT sustava, primjenom DevOps praksi uz korištenje alata CI/CD pipelines, Jenkins, Docker, Kubernetes, OpenShift Container Platform, u svojstvu stručnjaka za arhitekturu; minimalno jednom završenom projektu dizajniranja skalabilnih, modularnih i sigurnih sustava u svojstvu stručnjaka za arhitekturu.“ Tehnički stručnjak S4 - Stručnjak za programiranje - najmanje 1 (jedan) stručnjak. Stručnjak mora imati iskustvo u minimalno jednom završenom projektu s primjenom Java programiranja u kojem je stručnjak sudjelovao u svojstvu stručnjaka za programiranje. Tehnički stručnjak S5 - Stručnjak za baze podataka - najmanje 1 (jedan) stručnjak. Stručnjak mora imati iskustvo u minimalno jednom završenom projektu izrade baze podataka primjenom tehnologija Oracle, PostgreSQL, MySQL, PL/SQL, Docker, GitLab CI/CD, Ansible, Prometheus, Grafana i AWS, u svojstvu stručnjaka za baze podataka. Tehnički stručnjak S6 - Stručnjak za sistem administraciju – DevOPS - najmanje 1 (jedan) stručnjak. Stručnjak mora imati iskustvo u minimalno jednom završenom projektu izrade ili održavanja IT sustava primjenom tehnologija Oracle, PostgreSQL, MySQL, PL/SQL, Docker, GitLab CI/CD, Ansible, Prometheus, Grafana i AWS, u svojstvu stručnjaka za sistem administraciju. Tehnički stručnjak S7 - Serviser komunikacijske opreme - najmanje 1 (jedan) stručnjak. Stručnjak mora posjedovati važeće liječničko uvjerenje za rad na visini. Tehnički stručnjak S8 - Serviser komunikacijske opreme - najmanje 1 (jedan) stručnjak. Stručnjak mora posjedovati važeće liječničko uvjerenje za rad na visini.“ Točkom 5.2.2.5. propisan je način dokazivanja kao slijedi: „Za potrebe utvrđivanja okolnosti iz ove točke dokumentacije o nabavi gospodarski subjekt u ponudi kao preliminarni dokaz dostavlja ispunjeni ESPD obrazac. Po zahtjevu naručitelja za dostavu popratnih dokumenata, naručitelj će kao dovoljan dokaz radi dokazivanja sposobnosti gospodarskog subjekta prihvatiti Izjavu o stručnjacima koji će izvršavati ugovore zaključene na temelju okvirnog sporazuma u kojoj poimence moraju biti navedeni ponuđeni stručnjaci te iskustvo stručnjaka. Izjavi se prilažu važeći dokazi (certifikati, potvrde i sl.) o stručnoj osposobljenosti za tražene kompetencije.“

Uvidom u prijedlog okvirnog sporazuma članka 16. utvrđeno je da je u istome propisano kako slijedi: „U slučaju da su neki podaci označeni određenim stupnjem tajnosti (ograničeno) Naručitelj će o tome posebno obavijestiti Izvršitelja te zatražiti definiranje posebnog protokola za zaštitu navedenih podataka. Izvršitelj se obvezuje da će se kod pružanja ugovorene usluge iz ovog Okvirnog sporazuma ponašati u skladu sa propisanim mjerama i standardima informacijske sigurnosti i postupanja s klasificiranim i neklasificiranim podacima te da je upoznat s njima kao i sa zakonskim posljedicama u slučaju njihova nepridržavanja. Izvršitelj se obvezuje da će navedeno pravilo posebno primjenjivati na klasificirane i neklasificirane podatke i informacije kojima raspolaže Naručitelj u okviru svog djelokruga, a koji podaci su mu poznati ili mu postanu poznati tijekom realizacije ovog Okvirnog sporazuma i pružanju ugovorene usluge, a u vezi Naručiteljeve komunikacijske opreme i terminalnih uređaja i instalacija u funkciji komunikacija, financijskih podataka, podataka o postupcima nabave i drugih klasificiranih podataka, a čije bi neovlašteno ili/i neopravdano, umnožavanje, objavljivanje ili/i priopćavanje neovlaštenim osobama i trećima moglo nanijeti kakovu materijalnu ili nematerijalnu štetu ili/i moglo naštetiti sigurnosti, interesima i radu Naručitelja, Republici Hrvatskoj, ili/i fizičkim i pravnim osobama sa čijim klasificiranim podacima Naručitelj raspolaže u okviru svog djelokruga. Izvršitelj se obvezuje da će ispuniti sve propisane mjere i standarde za zaštitu klasificiranih i neklasificiranih podataka iz stavka 1. ovog članka Okvirnog sporazuma i da neće umnožavati, objaviti ili otkriti bilo usmeno, pismeno ili na bilo koji drugi način, neovlaštenoj osobi i trećima te podatke koje dobije ili kojima je imao ili ima pristup u tijeku izvršenja ovog Okvirnog sporazuma te da će u svezi zaštite klasificiranih i neklasificiranih podataka postupati sukladno odredbama Zakona o informacijskoj sigurnosti (Narodne novine, broj 79/07, 14/24), Zakona o tajnosti podataka (Narodne novine, broj 79/07 i 86/12), Zakona o

kibernetičkoj sigurnosti (Narodne novine, broj 14/24) i u skladu s Pravilnikom o tajnosti i zaštiti službenih podataka Ministarstva mora, prometa infrastrukture i Pravilnikom o provedbi mjera i standarda informacijske sigurnosti iz djelokruga rada Ministarstva mora, prometa i infrastrukture. Obveza čuvanja klasificiranih podataka i informacija u tajnosti ne prestaje prestankom važenja ovog Okvirnog sporazuma. Sve osobe koje će za Izvršitelja obavljati predmetne poslove iz ovog Okvirnog sporazuma moraju biti sigurnosno informirane i dužne su prije početka obavljanja tih poslova, kod Naručiteljevog Savjetnika za informacijsku sigurnost potpisati Izjavu o postupanju s klasificiranim podacima. Izvršitelj je dužan poduzimati preventivne mjere radi sprečavanja i otkrivanje zloupotrebe ili drugih neovlaštenih, štetnih ili neprimjerenih postupaka s klasificiranim i neklasificiranim podacima i informacijama od strane njegovih zaposlenika i drugih osoba koje angažira za obavljanje poslova iz ovog Ugovora. Izvršitelj se obvezuje da će čuvati kao poslovnu tajnu sve podatke bez obzira na njihovu vrstu i prirodu, a koji se odnose na Naručitelja i/ili njegove poslovne partnere, za koje je saznao na bilo koji način pružajući usluge koje su predmet ovog Okvirnog sporazuma Naručitelju. Izvršitelj se obvezuje obavljati poslove samo na temelju naloga Naručitelja, voditelja zbirke osobnih podataka. Izvršitelj se obvezuje čuvati osobne podatke zaposlenika Naručitelja i osobne podatke fizičkih osoba o kojima se vodi evidencija u bazama podataka te ih ne smije davati na korištenje drugim korisnicima, niti ih smije obrađivati za bilo koju drugu svrhu osim ugovorene. Izvršitelj se obvezuje osigurati provođenje odgovarajućih tehničkih, organizacijskih i kadrovskih mjera sukladno odredbama Zakona o provedbi opće Uredbe o zaštiti podataka (Narodne novine, broj 42/18). Izvršitelj se obvezuje raditi u okviru preporuka i tehničkih standarda koje određuje tijelo državne Uprave nadležno za informatizaciju Izvršitelj je dužan poduzimati preventivne mjere radi sprečavanja i otkrivanje zloupotrebe ili drugih neovlaštenih, štetnih ili neprimjerenih postupaka s klasificiranim i neklasificiranim podacima i informacijama od strane njegovih zaposlenika i drugih osoba koje angažira za obavljanje poslova iz ovog Ugovora. Izvršitelj se obvezuje da će čuvati kao poslovnu tajnu sve podatke bez obzira na njihovu vrstu i prirodu, a koji se odnose na Naručitelja i/ili njegove poslovne partnere, za koje je saznao na bilo koji način pružajući usluge koje su predmet ovog Okvirnog sporazuma Naručitelju. Izvršitelj se obvezuje obavljati poslove samo na temelju naloga Naručitelja, voditelja zbirke osobnih podataka. Izvršitelj se obvezuje čuvati osobne podatke zaposlenika Naručitelja i osobne podatke fizičkih osoba o kojima se vodi evidencija u bazama podataka te ih ne smije davati na korištenje drugim korisnicima, niti ih smije obrađivati za bilo koju drugu svrhu osim ugovorene. Izvršitelj se obvezuje osigurati provođenje odgovarajućih tehničkih, organizacijskih i kadrovskih mjera sukladno odredbama Zakona o provedbi opće Uredbe o zaštiti podataka (Narodne novine, broj 42/18). Izvršitelj se obvezuje raditi u okviru preporuka i tehničkih standarda koje određuje tijelo državne Uprave nadležno za informatizaciju.“

Uvidom u obavijest o provedenoj kategorizaciji subjekta Ureda Vijeća za nacionalnu sigurnost, KLASA: 200-01/25-02/123, URBROJ: 50439-04/42-25-04 od 20. ožujka 2025., koju je naručitelj dostavio u žalbenom postupku, utvrđeno je da je naručitelj identificiran kao ključan subjekt u smislu Zakona o kibernetičkoj sigurnosti (»Narodne novine«, broj 14/24.; dalje u tekstu: ZKS) za javni sektor i tijela državne uprave. Ujedno se navodi da je tijekom postupka kategorizacije provedena i nacionalna procjena kibernetičkih sigurnosnih rizika, pri čemu je za naručitelja utvrđena visoka razina kibernetičkih sigurnosnih rizika. Sukladno tome, naručitelj je obvezan provoditi naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima sukladno članku 42. stavku 3. i Prilogu II. Uredbe o kibernetičkoj sigurnosti („Narodne novine“, br. 135/24; dalje u tekstu: Uredba o kibernetičkoj sigurnosti).

Za ocjenu osnovanosti žalbenih navoda mjerodavno pravo čini odredba članka 256. stavak 1. ZJN 2016 kojim je propisano da se kriteriji za odabir gospodarskog subjekta u postupku javne nabave mogu odnositi na: sposobnost za obavljanje profesionalne djelatnosti; ekonomsku i financijsku sposobnost i tehničku i stručnu sposobnost. Stavkom 2. je propisano da javni naručitelj

smije kao uvjete sposobnosti gospodarskog subjekta u postupku javne nabave odrediti samo kriterije za odabir iz stavka 1. ovoga članka u skladu s odredbama ovoga odjeljka Zakona. Stavkom 3. je propisano da prilikom određivanja kriterija za odabir iz stavka 1. ovoga članka javni naručitelj smije zahtijevati samo minimalne razine sposobnosti koje osiguravaju da će gospodarski subjekt biti sposoban izvršiti ugovor o javnoj nabavi.

Dalje, člankom 12. stavkom 1. ZKS-a propisano je da se u kategoriju ključnih subjekata razvrstavaju, neovisno o njihovoj veličini: tijela državne uprave i druga državna tijela i pravne osobe s javnim ovlastima, ovisno o rezultatima provedene procjene njihove važnosti za nesmetano obavljanje ključnih društvenih ili gospodarskih djelatnosti. Člankom 25. stavkom 1. istoga zakona je propisano da zahtjevi kibernetičke sigurnosti obuhvaćaju postupke i mjere koje su ključni i važni subjekti dužni primjenjivati radi postizanja visoke razine kibernetičke sigurnosti u pružanju svojih usluga odnosno obavljanju svojih djelatnosti, a sastoje se od: mjera upravljanja kibernetičkim sigurnosnim rizicima i obveza obavještavanja o značajnim incidentima i ozbiljnim kibernetičkim prijetnjama. Stavkom 2. je propisano da se zahtjevi kibernetičke sigurnosti odnose se na *sve mrežne i informacijske sustave kojima se ključni i važni subjekti služe u svom poslovanju* ili u pružanju svojih usluga i sve usluge koje ključni i važni subjekti pružaju odnosno djelatnosti koje obavljaju, neovisno o tome pruža li subjekt i druge usluge odnosno obavlja li i druge djelatnosti koje nisu obuhvaćene Prilogom I. i Prilogom II. ZKS-a.

Nadalje, člankom 30. stavkom 1. ZKS-a je, između ostalog, propisano da se mjere upravljanja kibernetičkim sigurnosnim rizicima uključuju sigurnost lanca opskrbe, uključujući sigurnosne aspekte u pogledu odnosa između subjekta i njegovih izravnih dobavljača ili pružatelja usluga, dok je stavkom 3. propisano da će se mjere upravljanja kibernetičkim sigurnosnim rizicima i način njihove provedbe urediti uredbom iz članka 24. ZKS-a. Dalje, člankom 38. stavkom 2. trećom alinejom Uredbe o kibernetičkoj sigurnosti propisano je da se za visoku razinu procijenjenih kibernetičkih sigurnosnih rizika kategorizacijom subjekt obvezuje na provedbu napredne razine mjera upravljanja kibernetičkim sigurnosnim rizicima iz članka 42. stavka 3. i Priloga II. te Uredbe. Nadalje, u Prilogu II. Uredbe o kibernetičkoj sigurnosti, u okviru mjere 8. Sigurnost lanca opskrbe, točke 8.3., propisano je da sigurnosni zahtjevi mogu uključivati i odredbe o vještinama i osposobljavanju koje se zahtijevaju u odnosu na zaposlenike izravnog dobavljača ili pružatelja usluga te odredbe o certifikatima ili drugim ovlaštenjima koji se zahtijevaju za zaposlenike izravnog dobavljača ili pružatelja usluga.

Žalitelj osporava uvjete tehničke i stručne sposobnosti za stručnjake S1, S2, S3, S5 i S6, navodeći da tehničke specifikacije ne sadrže izrijekom aktivnosti, tehnologije i sigurnosna rješenja na koja se odnose tražena iskustva stručnjaka, zbog čega smatra da uvjeti nisu povezani niti razmjerni s predmetom nabave.

Naime, iz točke 3.1. dokumentacije o nabavi proizlazi da je predmet nabave održavanje RIS sustava sukladno troškovniku, tehničkoj specifikaciji i ostalim uvjetima dokumentacije o nabavi. Nadalje, iz tehničke specifikacije proizlazi da predmet nabave obuhvaća usluge preventivnog i korektivnog održavanja hrvatskog RIS sustava, pri čemu isti obuhvaća više funkcionalnih i tehničkih cjelina, uključujući uređaje i opremu, AIS informacijski sustav, VHF komunikacijski sustav, RIS aplikacijski sustav te podršku korisnicima. Naručitelj je u žalbenom postupku dodatno pojasnio da je RIS sustav dio integriranog informacijskog sustava naručitelja, da obuhvaća cijelu mrežu hrvatskih vodnih putova, ima međunarodnu povezanost i korisnike, zahtijeva neprekidnu dostupnost te visoku razinu zaštite od sve učestalijih i sofisticiranijih kibernetičkih prijetnji. Nadalje je naveo da sustav ispunjava uvjete povezivanja s europskim RIS sustavom koji ima više od 25.000 korisnika i koji obuhvaća 27.000 km plovnih putova, pri čemu navedene okolnosti prema ocjeni ovog tijela žalitelj tijekom postupka nije osporio.

S obzirom na navedeno, razvidno je da je predmet nabave složeni sustav koji je dio šireg integriranog i međunarodno povezanog informacijskog okvira, čije održavanje zahtijeva angažiranje stručnjaka s različitim kompetencijama radi osiguranja njegovog sigurnog i

kontinuiranog funkcioniranja. Naručitelj u svojim očitovanjima tijekom žalbenog postupka detaljno i jasno te iscrpno argumentira zahtjeve koje je postavio u odnosu na predmetne stručnjake, a koji zahtjevi su vezani za poduzimanje mjera upravljanja kibernetičkim sigurnosnim rizicima, a sve sukladno Zakonu o kibernetičkoj sigurnosti te Uredbi o kibernetičkoj sigurnosti, a temeljem kategorizacije naručitelja kao ključnog subjekta u smislu Zakona kibernetičkoj sigurnosti.

U tom smislu prihvaća se argumentacija naručitelja da se održavanje predmetnog sustava ne može promatrati izvan sigurnosnog i regulatornog okvira u kojem isti djeluje. Naime, iz članka 16. Prijedloga okvirnog sporazuma proizlazi da je izvršitelj obvezan postupati u skladu s mjerama i standardima informacijske sigurnosti te primjenjivim propisima iz područja informacijske i kibernetičke sigurnosti, uključujući obveze zaštite podataka, sprječavanja neovlaštenog pristupa te osiguravanja odgovarajućih tehničkih, organizacijskih i kadrovskih mjera zaštite informacijskog sustava i podataka kojima se u okviru izvršenja ugovora pristupa. Nadalje, iz obavijesti Ureda Vijeća za nacionalnu sigurnost od 20. ožujka 2025. proizlazi da je naručitelj kategoriziran kao ključni subjekt u smislu Zakona o kibernetičkoj sigurnosti te da je utvrđena visoka razina kibernetičkih sigurnosnih rizika, zbog čega je obvezan primjenjivati napredne mjere upravljanja kibernetičkim sigurnosnim rizicima. Slijedom navedenoga, prihvaća se argumentacija naručitelja da su zahtjevi vezani uz stručnjake iz područja informacijske sigurnosti, arhitekture informacijskih sustava, baza podataka i sistemske administracije povezani s njegovim zakonskim obvezama i sigurnosnim zahtjevima koji proizlaze iz važećeg regulatornog okvira.

S tim u vezi prihvaća se i argumentacija naručitelja da se uvjeti tehničke i stručne sposobnosti ne određuju isključivo prema trenutačno implementiranim funkcionalnostima sustava, već prema znanjima i iskustvima potrebnima za njegovo zakonito, sigurno i kvalitetno održavanje tijekom trajanja ugovora. Pri tome tehničke specifikacije određuju predmet i opseg usluge koja se održava, dok uvjeti tehničke i stručne sposobnosti služe provjeri raspolaže li gospodarski subjekt odgovarajućim stručnim kapacitetima za izvršenje ugovora. Stoga činjenica da pojedine tehnologije, alati ili sigurnosna rješenja nisu izričito navedeni u tehničkim specifikacijama ne znači da iskustvo u njihovoj primjeni nije povezano s predmetom nabave, a sve kako je to zbilja detaljno i jasno argumentirao naručitelj tijekom žalbenog postupka. Naime, predmetni uvjeti odnose se na dokazivanje tehničke i stručne sposobnosti gospodarskog subjekta te služi utvrđivanju njegove sposobnosti za kvalitetno i uredno izvršenje ugovora. Slijedom navedenoga, prema ocjeni ovog tijela predmetni uvjeti razmjerni su i povezani s predmetom nabave.

Nadalje, u odnosu na žalbene navode kojima se osporavaju pragovi od najmanje 1000 dnevnih korisnika, odnosno najmanje 200 dnevnih korisnika, prihvaća se argumentacija naručitelja da navedeni pragovi predstavljaju objektivne pokazatelje razine složenosti sigurnosnih izazova i zahtjevnosti sustava te razine iskustva potrebne za njegovo održavanje u uvjetima visoke dostupnosti i sigurnosne osjetljivosti. Ovdje je potrebno napomenuti da se ne radi o održavanju bilo kakvog sustava, već sustava čije održavanje se ne može promatrati izolirano od konteksta da se radi o sustavu naručitelja kao ključnog subjekta po kategorizaciji iz Zakona o kibernetičkoj sigurnosti, a što za sobom veže posljedice da je taj subjekt, obzirom na utvrđenu visoku razinu kibernetičkih sigurnosnih rizika obvezan provoditi naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima, a koje mjere se odnose na sve mrežne i informacijske sustave kojima se ključni i važni subjekti služe u svom poslovanju pa u tom smislu nije osnovan prigovor žalitelja da se te obveze ne odnose na RIS sustav. Tražene razine sposobnosti u konkretnom slučaju je naručitelj u tijeku žalbenog postupka detaljno i jasno argumentirao, dok s druge strane žalitelj prema ocjeni ovog nije dokazao da bi navedeni uvjeti sposobnosti bili nerazmjerni predmetu nabave, već se njegovi navodi temelje na usporedbi s ranijim ugovornim razdobljem.

U tom smislu ovo tijelo prihvaća argumentaciju naručitelja da se procjena potrebnih stručnih kapaciteta ne može temeljiti isključivo na ranijem stanju sustava, već i na sigurnosnim zahtjevima, razini rizika te potrebama sustava tijekom cijelog razdoblja izvršenja okvirnog sporazuma, a sve sukladno definiranim mjerama iz Priloga II Uredbe o kibernetičkoj sigurnosti.

Nisu osnovani niti žalbeni navodi kojima žalitelj ističe da se uvjeti za stručnjake S1 i S2 preklapaju. Naime, ovo je tijelo prihvatilo argumentaciju naručitelja da se radi o različitim stručnim profilima i skupovima kompetencija, pri čemu je potreba za više stručnjaka iz područja informacijske sigurnosti obrazložena složenošću sustava te obvezama koje proizlaze iz važećeg regulatornog okvira, osobito nakon stupanja na snagu Zakona o kibernetičkoj sigurnosti.

Nadalje, nisu osnovani niti žalbeni navodi kojima se osporava zahtjev da ponuditelj raspolaže s ukupno osam stručnjaka te da ista osoba ne može obavljati više funkcija. Iz točke 5.2.2.3 dokumentacije o nabavi proizlazi da je naručitelj taj zahtjev obrazložio opsegom i složenošću sustava, geografskom rasprostranjenošću te potrebom osiguravanja različitih stručnih područja za uredno i kontinuirano izvršenje ugovora. Slijedom navedenoga, prihvaća se argumentacija naručitelja da se radi o međusobno različitim stručnim ulogama koje zahtijevaju odvojene kompetencije, zbog čega nije nerazmjerno da ih obavljaju različite osobe.

Konačno, nije od utjecaja žaliteljevo pozivanje na ranije izvršavanje usluge održavanja RIS sustava niti na raniji postupak javne nabave, budući da su nastupile bitno izmijenjene okolnosti, osobito u pogledu regulatornog okvira iz područja kibernetičke sigurnosti te kategorizacije naručitelja kao ključnog subjekta s visokom razinom kibernetičkih sigurnosnih rizika. Stoga sama činjenica postojanja ranijeg ugovornog odnosa ne dovodi u pitanje ovlast naručitelja da u novom postupku odredi uvjete prilagođene važećim okolnostima.

Slijedom svega navedenoga, prema ocjeni ovog tijela, primjenom članka 403. stavka 1. o teretu dokazivanja, žalitelj nije dokazao da bi osporeni uvjeti tehničke i stručne sposobnosti bili određeni protivno članku 256. stavcima 3. i 4. ZJN 2016, radi čega se žalbeni navodi ocjenjuju neosnovanima.

Žalitelj dalje navodi da kriteriji za odabir ekonomski najpovoljnije ponude, kojima je naručitelj predvidio bodovanje specifičnog iskustva stručnjaka S1 i S2, nisu propisani sukladno članku 285. stavku 1. ZJN 2016. U tom smislu žalitelj ističe da je naručitelj u točki 3.4 dokumentacije o nabavi „Kriteriji za odabir ponuda“, kao i u dokumentu „Kriterij za odabir ekonomski najpovoljnije ponude“, odredio kriterije kvalitete kroz bodovanje specifičnog iskustva stručnjaka S1 i S2, pri čemu smatra da navedeni kriteriji nisu povezani s predmetom nabave te da pojedini od njih imaju diskriminirajući učinak. Navedene tvrdnje žalitelj temelji na analizi dokumentacije o nabavi i RIS sustava sadržanoj u Prilogu 1 žalbe, kao i na vlastitom iskustvu u održavanju predmetnog sustava u razdoblju od 2000. godine do lipnja 2024. godine. Žalitelj pritom navodi da tehničke specifikacije iz predmetnog postupka odgovaraju specifikacijama iz prethodnog ugovora o održavanju RIS sustava, slijedom čega zaključuje da u međuvremenu nisu izvršene značajnije nadogradnje niti uvedene nove funkcionalnosti sustava. Stoga smatra da raspolaže potrebnim stručnim saznanjima za ocjenu povezanosti propisanih kriterija s predmetom nabave.

U Prilogu I dostavljenom uz žalbu žalitelj u bitnome osporava zakonitost kriterija za odabir ekonomski najpovoljnije ponude u dijelu koji se odnosi na dodatno bodovanje iskustva stručnjaka S1 i S2, smatrajući da isti nisu određeni sukladno članku 285. stavku 1. ZJN 2016 se boduje iskustvo stručnjaka vezano za implementaciju rješenja koje nije sastavni dio RIS sustava, te iskustvo stručnjaka vezano za broj dnevnih korisnika koji značajno prelazi broj dnevnih korisnika RIS sustava. U odnosu na kriterije koji se odnose na implementaciju WAF rješenja, DoS i DDoS zaštite, sustava multifaktorske autentifikacije te sustava nadzora i zaštite baza podataka, žalitelj navodi da navedena rješenja nisu sastavni dio RIS sustava niti su predviđena tehničkim specifikacijama, koje uređuju isključivo održavanje postojećeg sustava. Također ističe da su u svim tim kriterijima propisani pragovi od najmanje 1000, odnosno 200 dnevnih korisnika, dok je broj registriranih korisnika RIS sustava u razdoblju 2020.–2024. godine bio 74, a u praksi se dnevno na sustav spajalo do najviše 10 korisnika, zbog čega smatra da su takvi pragovi nesrazmjerni stvarnom opsegu korištenja sustava i nejasni u pogledu načina dokazivanja.

Žalitelj dodatno ističe da je kriterij koji se odnosi na održavanje IT sigurnosnih sustava diskriminirajući, budući da se sigurnosni aspekti u dokumentaciji spominju isključivo u kontekstu organizacije održavanja opreme, bez definiranja konkretnih aktivnosti stručnjaka u tom području.

U odnosu na certifikat F5-401 – Security, žalitelj navodi da se radi o certifikatu koji se odnosi na tehnologije kompanije F5 Inc., koje nisu implementirane u RIS sustavu niti su obuhvaćene tehničkim specifikacijama, zbog čega smatra da se boduje specifično proizvođačko znanje koje nije povezano s predmetom nabave radi čeka je isto kriterij diskriminirajući.

U odnosu na S2 vezano za kriterije koji se odnose na razvoj i implementaciju strategije informacijske sigurnosti, vođenje tima za sigurnost informacijskih sustava te upravljanje sigurnosnim incidentima i procjenu rizika, žalitelj navodi da tehničke specifikacije ne predviđaju takve aktivnosti, već isključivo održavanje sustava, zbog čega smatra da navedeno iskustvo nije relevantno za predmet nabave. Nadalje, u odnosu na kriterije koji se odnose na implementaciju SOAR rješenja i zaštitu baze podataka, žalitelj ističe da takva rješenja nisu sastavni dio RIS sustava niti su obuhvaćena tehničkim specifikacijama, pa se boduje iskustvo koje nije povezano s predmetom nabave. U odnosu na kriterij koji se odnosi na posjedovanje CISSP certifikata, žalitelj navodi da se radi o certifikatu iz područja kibernetičke sigurnosti, dok tehničke specifikacije ne obuhvaćaju aktivnosti stručnjaka u tom području, već isključivo održavanje sustava, zbog čega smatra da ni taj kriterij nije povezan s predmetom nabave te da je diskriminirajući.

Naručitelj u odgovoru na žalbu navodi da je RIS sustav dio šireg i kritičnog informacijskog sustava naručitelja, zbog čega smatra opravdanim, proporcionalnim i s predmetom nabave povezanim vrednovanje specifičnog iskustva stručnjaka S1 i S2. Dalje navodi da su kriteriji kojima se vrednuje iskustvo stručnjaka S1 i S2 povezani s predmetom nabave jer su usmjereni na upravljanje ključnim sigurnosnim i operativnim rizicima RIS sustava, osobito u dijelu: zaštite sustava od kibernetičkih prijetnji, uključujući WAF zaštitu, zaštitu od DoS/DDoS napada, autentifikaciju korisnika i zaštitu baza podataka; rastućih zahtjeva europske RIS mreže s tisućama korisnika i obveza koje proizlaze iz propisa o kibernetičkoj sigurnosti. Nadalje, naručitelj ističe da iskustvo stručnjaka S1 i S2 predstavlja objektivno mjerljivu i relevantnu okolnost koja izravno utječe na funkcionalnost, sigurnost i pouzdanost održavanja sustava. Također navodi da se vrednovanjem dodatnog iskustva stručnjaka S1 i S2 ne propisuju uvjeti sposobnosti odnosno uvjeti za sudjelovanje u postupku javne nabave, već kriteriji za odabir ekonomski najpovoljnije ponude, kojima se nastoji osigurati viša kvaliteta ponude i viša razina stručnosti i sigurnosti, što može imati značajan utjecaj na uspješnost izvršenja ugovora.

Žalitelj u podnesku od 22. listopada 2025. navodi da je svjestan kako kriteriji za odabir ekonomski najpovoljnije ponude daju naručitelju opciju bodovanja više razine kvalitete i da oni nisu minimalni uvjet za sudjelovanje. Međutim, žalitelj smatra da je i u tom slučaju naručitelj, sukladno članku 285. stavku 1. ZJN 2016, obvezan propisati kriterije koji su povezani s predmetom nabave. Nadalje navodi da se naručitelj u svom očitovanju osvrnuo samo na manji dio žalbenih navoda, odnosno njihove detaljne razrade iz Priloga 1, dok se uopće nije očitovao na analizu većine kriterija kvalitete za stručnjake S1 i S2 niti je dostavio podatke i dokaze kojima bi dokazao da su traženi kriteriji povezani s predmetom nabave. U tom smislu žalitelj ponovno ukazuje na kriterije povezane s brojem korisnika nacionalnog RIS sustava te na iskustvo u razvoju i implementaciji strategije informacijske sigurnosti. Vezano uz broj korisnika, žalitelj navodi da je naručitelj samo paušalno ukazao na rastuće zahtjeve europske RIS mreže s tisućama korisnika, pri čemu ponovno ističe da se predmet nabave odnosi isključivo na održavanje nacionalnog RIS sustava. Nadalje navodi da naručitelj nije osporio žaliteljeve tvrdnje da nacionalni RIS sustav nema traženih 1000 odnosno 200 dnevnih korisnika, već višestruko manji broj korisnika od onoga predviđenog predmetnim kriterijima. Nadalje, žalitelj ističe da se naručitelj i u odnosu na pozivanje na Zakon o kibernetičkoj sigurnosti poziva na okolnosti koje, prema mišljenju žalitelja, nisu povezane s opisom predmeta nabave.

Naručitelj u podnesku od 28. siječnja 2026. u bitnome navodi da žalitelj pogrešno i preusko tumači zahtjev povezanosti kriterija s predmetom nabave iz članka 285. stavka 1. ZJN 2016. Prema stajalištu naručitelja, kriterij je povezan s predmetom nabave ako se odnosi na način izvršenja ugovora te utječe na kvalitetu, pouzdanost, sigurnost ili učinkovitost pružene usluge, odnosno ako doprinosi smanjenju operativnih, tehničkih i sigurnosnih rizika tijekom izvršenja ugovora. Slijedom navedenoga, naručitelj smatra da kriteriji ne moraju predstavljati doslovno ponavljanje tehničkih specifikacija ili opisa usluge, već mogu biti usmjereni na kvalitativne aspekte izvršenja ugovora, što je, prema navodima naručitelja, slučaj u predmetnom postupku.

Nadalje, naručitelj osporava tvrdnju žalitelja da se nije očitovao na većinu kriterija za stručnjake S1 i S2 te navodi da je očitovanje dano sažeto i usmjereno na bitne navode. Ističe i da je naknadno dostavio dodatno pojašnjenje kojim su detaljnije obrazloženi razlozi propisivanja kriterija za dodatno iskustvo S1 i S2. U tom smislu naručitelj navodi da se predmetni kriteriji temelje na činjenici da je RIS sustav dio kritičnog informacijskog okruženja, na obvezi osiguravanja visoke razine informacijske sigurnosti te na potrebi upravljanja sigurnosnim i operativnim rizicima koji, prema mišljenju naručitelja, proizlaze iz stvarne naravi i učinaka sustava, a ne isključivo iz formalnog opisa predmeta nabave. Naručitelj ističe da kriteriji kvalitete nisu određeni proizvoljno, već radi razlikovanja ponuda prema sposobnosti ponuditelja da preventivno upravlja sigurnosnim incidentima, odgovori na složene prijetnje i osigura stabilnost sustava tijekom trajanja okvirnog sporazuma.

U odnosu na navode žalitelja vezane uz broj korisnika sustava, naručitelj navodi da žalitelj pogrešno polazi od pretpostavke da je broj korisnika relevantan isključivo kao trenutačni statistički podatak nacionalnog RIS sustava. Naručitelj ističe da se kriterij broja korisnika koristi kao objektivni pokazatelj složenosti sustava, iskustva stručnjaka u radu s visokodostupnim sustavima te sposobnosti upravljanja sigurnošću, performansama i incidentima u okruženjima s većim opterećenjem. Ističe da se stvarne karakteristike sustava ne određuju se samo brojem korisnika iz nekog razdoblja, nego razinom izloženosti prijetnjama, važnošću podataka, zahtjevima 24/7 dostupnosti te ulogom sustava u sigurnosti plovidbe i međunarodnoj razmjeni podataka. Prema navodima naručitelja, činjenica da nacionalni RIS sustav trenutačno nema 1000 odnosno 200 dnevnih korisnika ne utječe na legitimnost predmetnog kriterija, budući da održavanje sustava obuhvaća i postupanje u uvjetima vršnih opterećenja, izvanrednih situacija i budućeg razvoja sustava.

Nadalje, naručitelj osporava i navod žalitelja da iskustvo u razvoju i implementaciji strategije informacijske sigurnosti nije povezano s predmetom nabave. U tom smislu navodi da održavanje RIS sustava ne obuhvaća samo tehničke intervencije, već i kontinuiranu procjenu sigurnosnih prijetnji, prilagodbu sigurnosnih mjera te upravljanje incidentima i ranjivostima sustava. Stoga smatra da iskustvo u izradi i provedbi sigurnosnih strategija izravno utječe na način izvršenja ugovora, povećava otpornost sustava te smanjuje rizik zastoja i kompromitacije podataka. Zaključno, naručitelj navodi da kriteriji za odabir ponude ne zahtijevaju da svaka zakonska obveza bude izrijekom navedena u tehničkim specifikacijama, već da je dovoljno da kriteriji adresiraju rizike i zahtjeve koji proizlaze iz zakonodavnog okvira u kojem se ugovor izvršava. Također ponavlja da dodatno iskustvo stručnjaka S1 i S2 ne predstavlja uvjet za sudjelovanje u postupku, već kriterij kvalitete kojim se omogućuje odabir ekonomski najpovoljnije ponude s višom razinom stručnosti i sigurnosti.

U prilogu koji je naručitelj dostavio uz podnesak dodatno, u bitnome pojašnjava, da su kriteriji kvalitete koji se odnose na organizaciju, kvalifikacije i iskustvo stručnjaka koje će izvršavati ugovor opravdani kada takvi kriteriji mogu utjecati na razinu kvalitete izvršenja ugovora, sukladno članku 285. stavku 1. ZJN 2016. U predmetnom slučaju bodovanje se odnosi isključivo na dodatno iskustvo stručnjaka te ne uvodi nove obveze, ne proširuje predmet nabave i ne mijenja njegov opseg. Iskustvo stručnjaka koje se boduje izravno je povezano s kvalitetom i sigurnošću izvršenja

usluge održavanja informacijskog sustava, pri čemu sigurnost predstavlja ključni element funkcioniranja i održavanja RIS sustava.

U odnosu na žalbeni navod da je kriterij kojim se vrednuje iskustvo u održavanju IT sigurnosnih sustava diskriminirajući i nepovezan s predmetom nabave, naručitelj je mišljenja da je korištenje kriterija koji se odnose na iskustvo i osposobljenost stručnjaka i kojim se boduje iskustvo stručnjaka u održavanju IT sigurnosnih sustava izravno povezan s predmetom nabave, da se odnosi na kvalitetu izvršenja ugovora te da vrednuje iskustvo stručnjaka koji će sudjelovati u održavanu RIS sustava. Također navodi da navedeni kriterij doprinosi višoj razini kvalitete izvršenja ugovora dok u konkretnom slučaju, viša razina sigurnosne stručnosti smanjuje operativne i sigurnosne rizike, povećava pouzdanost održavanja, te doprinosi stabilnosti i dostupnosti RIS sustava. Nadalje, navodi da navedeni kriterij nije uvjet za sudjelovanje u postupku, ne isključuje nijednog gospodarskog subjekta, primjenjuje se jednako na sve ponuditelje i služi isključivo za razlikovanje ponuda prema razini kvalitete. Ujedno ističe da bodovanje do najviše 10 projekata omogućuje proporcionalno vrednovanje dodatnog iskustva, sprječava neograničeno bodovanje, osigurava razmjernost i transparentnost.

Nadalje, ističe da posjedovanje F5 certifikata nije propisano kao obvezan uvjet za sudjelovanje u postupku nabave, već predstavlja element koji se vrednuje u okviru kriterija za odabir ponude. Stoga okolnost da pojedini gospodarski subjekt ne raspolaže navedenim certifikatom ne sprječava njegovo sudjelovanje u postupku niti podnošenje valjane i konkurentne ponude. Bodovanje posjedovanja F5 certifikata koristi se isključivo kao pokazatelj razine sigurnosne stručnosti, bez stvaranja tehnološke ovisnosti o jednom proizvođaču. Dalje navodi da CISSP certifikat nije vezan uz jednog proizvođača ili tehnologiju, međunarodno je priznat i dostupan svim stručnjacima pod jednakim uvjetima, te da bodovanje posjedovanja navedenog certifikata ne ograničava tržišno natjecanje, već potiče kvalitetu. Certifikat se temelji na neutralnim sigurnosnim principima, međunarodnim normama i najboljim praksama primjenjivima na bilo koji informacijski sustav, uključujući RIS.

Naručitelj dodatno ističe da je kriterij „minimalno 1000 dnevnih korisnika", odnosno „minimalno 200 dnevnih korisnika", jasno definiran kao objektivni i mjerljivi prag kojim se iskazuje razina složenosti i opterećenja referentnog sustava u kojem je stručnjak stekao iskustvo, te ne zahtijeva dodatno normiranje u tehničkim specifikacijama.

Ocjenjujući žalbeni navod utvrđeno je slijedeće činjenično stanje. Uvidom u dokumentaciju o nabavi u dijelu Kriterij za odabir najpovoljnije ponude utvrđeno je da se u istoj navodi: „Kriterij odabira je ekonomski najpovoljnija ponuda. Naručitelj će primjenom apsolutnog modela za ocjenu ponude temeljem ponuđenog iskustva stručnjaka utvrditi usporednu cijenu za svaku ponudu. Za sklapanje ugovora primjenjivat će se cijene navedene u troškovniku od strane ponuditelja. Ponuda s ukupnom (usporednom) najnižom cijenom prema kriterijima bit će izabrana kao najpovoljnija. S obzirom na to da ne može koristiti pravo na pretporez, naručitelj će uspoređivati cijene ponuda s PDV-om. Ako dvije ili više ponuda budu jednako rangirane prema kriteriju za odabir ponude, naručitelj će odabrati ponudu koja je zaprimljena ranije. Ekonomski najpovoljnija ponuda utvrditi će se temeljem sljedećih kriterija: 1. Cijena ponude 2. Kvaliteta – specifično iskustvo stručnjaka"… „a) Cijena (CP) Cijena ponude je ponuđena cijena ponuditelja sukladno troškovniku. Od ponuđene cijene s PDV-om oduzimaju se apsolutne vrijednosti odnosno iznosi koje ponuda ostvari temeljem kvalitativnih kriterija. Iznos dobiven na taj način predstavlja usporednu cijenu ponude. Naručitelj će odabrati ponudu koja ima najnižu usporednu cijenu. b) Kvaliteta Jedna osoba može biti imenovana na jednu poziciju."…" Specifično iskustvo stručnjaka za sigurnost informacijskih sustava br. 1 (S1) Naručitelj će ponudama u kojima se nudi stručnjak s iskustvom povrh minimalno zahtijevanog umanjiti ponuđenu cijenu. Cijena će se umanjivati za iskustvo rada na projektima na kojima je stručnjak sudjelovao u svojstvu stručnjaka za sigurnost informacijskih sustava. Za svaki završeni projekt implementacije WAF rješenja za zaštitu web aplikacija na softverima za minimalno 1000 dnevnih korisnika naručitelj će umanjiti cijenu ponude za 4.000,00 EUR po projektu do najviše

20.000,00 EUR za 5 projekata. Za svaki završeni projekt implementacije DoS i DDoS rješenja na softverima za minimalno 1000 dnevnih korisnika naručitelj će umanjiti cijenu ponude za 4.000,00 EUR po projektu do najviše 20.000,00 EUR za 5 projekata. Za svaki završeni projekt implementacije sustava za multi faktorsku autentifikaciju na softverima za minimalno 200 dnevnih korisnika naručitelj će umanjiti cijenu ponude za 4.000,00 EUR po projektu do najviše 20.000,00 EUR za 5 projekata. Za svaki završeni projekt implementacije sustava za nadzor i zaštitu baze podataka na softverima za minimalno 1000 dnevnih korisnika naručitelj će umanjiti cijenu ponude za 5.000,00 EUR po projektu do najviše 15.000,00 EUR za 3 projekta. Za svaki završeni projekt održavanja IT sigurnosnih sustava naručitelj će umanjiti cijenu ponude za 1.000,00 EUR po projektu do najviše 10.000,00 EUR za 10 projekata. Ako navedeni stručnjak posjeduje važeći certifikat za primjenu sigurnosnih rješenja (F5-401 – Security) naručitelj će umanjiti cijenu ponude za dodatnih 5.000,00 EUR“ i „ Specifično iskustvo stručnjaka za sigurnost informacijskih sustava br. 2 (S2) Naručitelj će ponudama u kojima se nudi stručnjak s iskustvom povrh minimalno zahtijevanog umanjiti ponuđenu cijenu. Cijena će se umanjivati za iskustvo rada na projektima na kojima je stručnjak sudjelovao u svojstvu stručnjaka za sigurnost informacijskih sustava. Za svaki završeni projekt iz područja implementacije sustava informacijske sigurnosti naručitelj će umanjiti cijenu ponude za 2.000,00 EUR po projektu do najviše 20.000,00 EUR za 10 projekata. Za svaki završeni projekt razvoja i implementacije strategije informacijske sigurnosti naručitelj će umanjiti cijenu ponude za 5.000,00 EUR po projektu do najviše 15.000,00 EUR za 3 projekta. Za svaki završeni projekt u kojem je stručnjak sudjelovao u svojstvu voditelja tima za sigurnost informacijskih sustava naručitelj će umanjiti cijenu ponude za 2.000,00 EUR po projektu do najviše 20.000,00 EUR za 10 projekata. Za svaki završeni projekt upravljanja sigurnosnim incidentima i procjenom rizika naručitelj će umanjiti cijenu ponude za 4.000,00 EUR po projektu do najviše 20.000,00 EUR za 5 projekata. Za svaki završeni projekt implementacije zaštite baze podataka naručitelj će umanjiti cijenu ponude za 10.000,00 EUR po projektu do najviše 20.000,00 EUR za 2 projekta. Za svaki završeni projekt implementacije SOAR rješenja naručitelj će umanjiti cijenu ponude za 10.000,00 EUR po projektu do najviše 20.000,00 EUR za 2 projekta. Ako navedeni stručnjak posjeduje važeći CISSP certifikat naručitelj će umanjiti cijenu ponude za dodatnih 5.000,00 EUR.“

Za ocjenu osnovanosti žalbenog navoda mjerodavno pravo čine odredbe članka 285. stavka 1. ZJN 2016 kojima je propisano da kriteriji za odabir ponude ne smiju biti diskriminirajući, moraju biti povezani s predmetom nabave te moraju omogućiti učinkovito nadmetanje.

Uvidom u dokumentaciju o nabavi, u dijelu „Kriteriji za odabir ponuda“ te u dokumentu „Kriterij za odabir ekonomski najpovoljnije ponude“, utvrđeno je da je naručitelj propisao da se ekonomski najpovoljnija ponuda utvrđuje primjenom apsolutnog modela bodovanja, pri čemu se kvalitativni kriterij odnosi na specifično iskustvo stručnjaka S1 i S2. Navedeno iskustvo vrednuje se kroz prethodno provedene projekte u području sigurnosti informacijskih sustava te posjedovanje određenih certifikata, uz unaprijed definirane iznose umanjenja cijene po pojedinom projektu i maksimalne pragove bodovanja.

Žalitelj osporava zakonitost predmetnih kriterija navodeći da isti nisu povezani s predmetom nabave, koji se prema njegovom tumačenju odnosi isključivo na održavanje RIS sustava, te da se bodovanjem obuhvaćaju iskustva stručnjaka koja se odnose na implementaciju rješenja koja nisu dio predmetnog sustava, kao i iskustva vezana uz sustave i tehnologije koji prema njegovim navodima nisu implementirani u RIS sustav. Nadalje, žalitelj tvrdi da kriteriji koji se odnose na broj dnevnih korisnika nisu razmjerni jer ne odgovaraju stvarnom opsegu korištenja nacionalnog RIS sustava. Također, žalitelj navodi da određeni kriteriji, uključujući bodovanje za specifične certifikate F5-401 i CISSP te za iskustvo u određenim IT rješenjima, imaju diskriminirajući učinak jer, prema njegovom stajalištu, ne dopuštaju svim potencijalnim ponuditeljima jednake uvjete natjecanja.

Međutim, takvi navodi žalitelja, prema ocjeni ovog tijela nisu osnovani.

U okviru ocjene prvog žalbenog navoda već je utvrđeno da je RIS sustav dio integriranog informacijskog sustava naručitelja, povezan s drugim državnim i međunarodnim informacijskim sustavima, da djeluje u okviru europskog RIS okvira koji ima više od 25.000 korisnika te da obuhvaća mrežu plovnih putova od približno 27.000 km, pri čemu je naručitelj ujedno ključni subjekt u nacionalnom informacijskom sustavu i, sukladno Zakonu o kibernetičkoj sigurnosti, obveznik osiguravanja visoke razine informacijske sigurnosti svojih sustava. Slijedom tako utvrđenih okolnosti, prihvaća se argumentacija naručitelja da se predmet nabave odnosi na složen, umrežen i kritičan informacijski sustav čije održavanje, po svojoj prirodi, zahtijeva visoku razinu sigurnosti, otpornosti i operativne pouzdanosti, kao i angažiranje stručnjaka s odgovarajućim kompetencijama za upravljanje sigurnosnim i operativnim rizicima, uključujući zaštitu od kibernetičkih prijetnji.

Polazeći od navedenog, prihvaća se stajalište naručitelja da se iskustvo koje se boduje kao dio kriterija za odabir ponude ne mora ograničiti isključivo na elemente koji su doslovno opisani tehničkim specifikacijama kao dio RIS sustava, već mogu obuhvaćati i dodatna stručna iskustva koja su objektivno povezana s kvalitetom izvršenja ugovora, osobito u slučaju sustava koji zahtijeva visoku razinu informacijske sigurnosti i zaštite od kibernetičkih napada. Stoga činjenica da pojedina tehnička rješenja ili aktivnosti nisu izrijekom navedene u tehničkim specifikacijama sama po sebi ne isključuje njihovu povezanost s predmetom nabave, ako iz prirode sustava i svrhe ugovora proizlazi potreba za takvim kompetencijama, kako to osnovano ističe i detaljno u okviru žalbenog postupka argumentira naručitelj.

Nadalje, u odnosu na kriterije koji se odnose na broj dnevnih korisnika, prihvaća se obrazloženje naručitelja da se propisani pragovi od 1000 odnosno 200 korisnika ne odnose na stvarni broj korisnika nacionalnog RIS sustava, već predstavljaju objektivni pokazatelj složenosti i opterećenja sustava u referentnim projektima u kojima je stručnjak stjecao iskustvo. Takav kriterij služi kao mjerilo iskustva u radu s visokodostupnim sustavima i okruženjima povećanog opterećenja te omogućuje vrednovanje sposobnosti upravljanja sigurnosnim i operativnim izazovima u takvim uvjetima, kako to osnovano navodi naručitelj te je u skladu s rastućim zahtjevima europske RIS mreže s tisućama korisnika kao i obvezama koje za naručitelja proizlaze iz propisa o kibernetičkoj sigurnosti. Slijedom navedenog prema ocjeni ovog tijela sama činjenica da nacionalni RIS sustav eventualno ima manji broj korisnika ne dovodi u pitanje zakonitost predmetnog kriterija, osobito uzimajući u obzir da je RIS sustav dio europskog RIS okvira koji ima više od 25.000 korisnika, a što je već detaljno obrazloženo u ocjeni prethodnog žalbenog navoda.

U odnosu na žalbene navode kojima žalitelj osporava kriterije koji se odnose na posjedovanje certifikata F5-401 i CISSP te na iskustvo stručnjaka u području IT sigurnosnih rješenja, naručitelj je tijekom žalbenog postupka pojasnio da se navedeni kriteriji odnose na iskustvo i osposobljenost stručnjaka koji će sudjelovati u održavanju RIS sustava te da izravno doprinose kvaliteti izvršenja ugovora kroz smanjenje operativnih i sigurnosnih rizika, povećanje pouzdanosti održavanja te osiguravanje stabilnosti i dostupnosti sustava. Također je naveo da certifikati F5-401 i CISSP nisu propisani kao obvezni uvjeti za sudjelovanje u postupku, već se vrednuju isključivo u svrhu ostvarivanja dodatnih bodova u okviru kriterija za odabir ekonomski najpovoljnije ponude. Naručitelj jasno argumentira da se bodovanje posjedovanja F5 certifikata koristi isključivo kao pokazatelj razine sigurnosne stručnosti, bez stvaranja tehnološke ovisnosti o jednom proizvođaču kao i da CISSP certifikat nije vezan uz jednog proizvođača ili tehnologiju, međunarodno je priznat i dostupan svim stručnjacima pod jednakim uvjetima, te da bodovanje posjedovanja navedenog certifikata ne ograničava tržišno natjecanje, već potiče kvalitetu. Pri ocjeni ovog žalbenog navoda osobito je uzet u obzir, u odnosu na konkretan predmet nabave i citirani sadržaj Uredbe o kibernetičkoj sigurnosti koja u Prilogu II. definira napredne razine mjera upravljanja kibernetičkim sigurnosnim rizicima (čiji je naručitelj obveznik) te pritom u okviru mjere 8. Sigurnost lanca opskrbe, točke 8.3., propisuje da sigurnosni zahtjevi mogu uključivati i odredbe o certifikatima ili drugim ovlaštenjima koji se zahtijevaju za zaposlenike izravnog dobavljača ili pružatelja usluga.

Naručitelj pritom dodatno argumentira i da sporni kriteriji nisu propisani kao uvjeti sposobnosti niti njihovo neispunjavanje dovodi do isključenja ponuditelja iz postupka, već predstavljaju elemente koji čine dodatnu kvalitetu za dodatno bodovanje ponuda. Slijedom navedenog, ne može se prihvatiti žalbeni navod da je riječ o kriterijima koji nisu vezani za predmet nabave ili diskriminiraju gospodarske subjekte.

Slijedom svega navedenog, ocjenjuje se da osporeni kriteriji u konkretnom slučaju nisu propisani protivno ZJN 2016 budući da su povezani s predmetom nabave i nisu diskriminirajući u smislu članka 285. stavka 1. ZJN 2016, te su stoga žalbeni navodi ocijenjeni neosnovanima.

Žalitelj dalje navodi da je naručitelj u dokumentaciji o nabavi pod točkom 5.2 Tehnička i stručna sposobnost odredio uvjet 5.2.2 Tehnički stručnjaci ili tijela – kontrola kvalitete, pri čemu su za S1 propisani uvjeti iskustva koji uključuju odrednicu „broj dnevnih korisnika“, i to na način da se traži minimalno jednom završen projekt implementacije WAF rješenja za zaštitu web aplikacija na softverima za minimalno 1000 dnevnih korisnika, minimalno jednom završen projekt implementacije DoS i DDoS rješenja na softverima za minimalno 1000 dnevnih korisnika, minimalno jednom završen projekt implementacije sustava za multifaktorsku autentifikaciju na softverima za minimalno 200 dnevnih korisnika te minimalno jednom završen projekt implementacije sustava za nadzor i zaštitu baze podataka na softverima za minimalno 1000 dnevnih korisnika, pri čemu se isti pojam „minimalni broj dnevnih korisnika“ koristi i u točki 3.4 Kriteriji za odabir ponuda u dijelu koji se odnosi na bodovanje specifičnog iskustva stručnjaka S1. Uz žalbene navode br. 1. koji se odnosi na nepovezanost i nerazmjernost s predmetom nabave te br. 2. koji se odnosi na nezakonitost kriterija za odabir ponude, žalitelj smatra da ovakve odredbe nisu u skladu s člankom 200. stavkom 1. ZJN 2016.

Žalitelj u Prilogu 1 navodi niz karakteristika i funkcionalnosti koje RIS sustav ne sadrži, kao i vrsta usluga koje nisu opisane u tehničkim specifikacijama, a u odnosu na koje se traži relevantno iskustvo stručnjaka ili se iste vrednuju kroz kriterije za odabir ponude. Ističe da, čak i kada bi pojedine od tih karakteristika ili usluga bile dio RIS sustava ili predmetne usluge, tehničke specifikacije ne sadržavaju jasne reference na njih. Stoga smatra da je dokumentacija o nabavi nejasna i neprecizna te da ne omogućuje podnošenje usporedivih ponuda, osobito imajući u vidu da se predmet nabave odnosi na uslugu održavanja sustava, zbog čega gospodarski subjekti moraju biti upoznati sa svim glavnim karakteristikama i funkcionalnostima sustava kako bi mogli izraditi realne i usporedive ponude.

Nadalje, žalitelj smatra da se svi aspekti koji su dokumentacijom propisani kao minimalni uvjeti ili kriteriji za odabir ponude moraju smatrati glavnim karakteristikama i funkcionalnostima sustava, odnosno bitnim elementima predmetne usluge, jer bi u protivnom njihovo propisivanje bilo bespredmetno. Prema njegovom stajalištu, dokumentacija se može smatrati jasnom i preciznom samo ako tehničke specifikacije sadržavaju jasne reference na takve elemente, što u konkretnom slučaju, prema navodima žalitelja, nije ispunjeno.

Dodatno, žalitelj smatra da dokumentacija nije jasna ni precizna jer nije određeno na koji će se način utvrđivati minimalni broj dnevnih korisnika sustava. Navodi da nije razjašnjeno radi li se o registriranom dnevnom broju korisnika, prosječnom dnevnom broju korisnika na godišnjoj razini, minimalnom broju korisnika ostvarenome tijekom svakog dana korištenja sustava ili nekoj drugoj metodologiji. Zbog mogućnosti različitih tumačenja smatra da gospodarski subjekti nisu u mogućnosti izraditi usporedive ponude niti sa sigurnošću predvidjeti način vrednovanja svojih referenci.

Naručitelj u odgovoru na žalbu navodi da su opisom predmeta nabave i tehničkim specifikacijama navedene sve okolnosti relevantne za izradu ponude te osigurana usporedivost pristiglih ponuda u odnosu na postavljene uvjete i zahtjeve. Ističe da se prilikom izrade dokumentacije pridržavao načela javne nabave sukladno članku 4. ZJN 2016. Pojam „dnevni korisnici“, koji s u kontekstu informacijskih sustava i IT infrastrukture, koristi se za evaluaciju opsega i kompleksnosti sigurnosnih mjera, procjenu učinkovitosti implementiranih rješenja u stvarnim uvjetima te razlikovanje iskustva s manjim, zatvorenim sustavima i onih s većim brojem

krajnjih korisnika. Dokazivanje kriterija u smislu broja dnevnih korisnika jasno je mjerljivo, primjerice putem potvrda, dokumentacije projekta, tehničkih opisa i slično.

Žalitelj u podnesku od 22. listopada 2025. smatra da opis predmeta nabave i tehnička specifikacija ne sadrže sve okolnosti koje su značajne za izradu ponude te za usporedivost pristiglih ponuda u pogledu postavljenih uvjeta i zahtjeva. Na to, prema njegovom stavu, upućuje i sam odgovor naručitelja, u kojem se navode dodatne karakteristike i zahtjevi, prvenstveno oni temeljeni na Zakonu o kibernetičkoj sigurnosti, a koji nisu izrijekom navedeni u dokumentaciji o nabavi. Nadalje, žalitelj ističe da naručitelj ni u odgovoru nije razjasnio pojam „dnevnih korisnika“ niti način njegova određivanja, odnosno metodologiju prema kojoj bi gospodarski subjekti trebali dokazivati takav podatak u okviru referenci stručnjaka. Smatra da naručitelj nije naveo niti podatak o stvarnom broju dnevnih korisnika RIS sustava, čime bi se, prema njegovom mišljenju, mogla dokazati povezanost uvjeta sposobnosti i kriterija za odabir s predmetom nabave.

Naručitelj u podnesku od 28. siječnja 2026. navodi da ZJN 2016 ne zahtijeva da dokumentacija sadrži sve interne tehničke, organizacijske i sigurnosne okolnosti naručitelja, niti da se detaljno obrazlažu svi regulatorni razlozi postavljanja određenih uvjeta i kriterija, kao ni da se navode operativni podaci koji nisu dio predmeta ugovora, već služe kao pokazatelj složenosti sustava. Naručitelj osporava tvrdnju žalitelja da opis predmeta nabave i tehničke specifikacije ne sadržavaju sve bitne okolnosti, navodeći da je u odgovoru sažeto i sistematično prikazao relevantne elemente, te dodatno, kroz prošireni odgovor na pojedinačne navode žalbe, jasno obrazložio da dokumentacija definira predmet nabave – održavanje RIS sustava, precizira vrstu usluga, određuje minimalne uvjete sposobnosti i kriterije za odabir ponude te omogućuje gospodarskim subjektima da nedvojbeno razumiju opseg i složenost ugovora. Dalje navodi da obveze iz Zakona o kibernetičkoj sigurnosti, ne predstavljaju dodatne zahtjeve, već čine pravni okvir izvršenja ugovora i objektivne činjenice koje postoje neovisno o dokumentaciji, pri čemu pozivanje na zakone ne dovodi u pitanje jasnoću dokumentacije, nego potvrđuje njezinu zakonitost. Što se tiče pojma „dnevni korisnici“, naručitelj navodi da se radi o standardnom pojmu u području informacijskih sustava koji služi za procjenu opsega, opterećenja i složenosti sustava te razlikovanje iskustva na manjim i zatvorenim sustavima od iskustva na sustavima s većim brojem korisnika. Ističe da je način dokazivanja tog podatka objektivan i provjerljiv te da se može dokazivati kroz projektne reference, tehničke opise, potvrde naručitelja i drugu relevantnu dokumentaciju. Dokumentacija o nabavi, prema stavu naručitelja, ne mora propisivati jedinstvenu metodologiju dokazivanja svakog tehničkog podatka, već je dovoljno da su zahtjevi objektivni, razumljivi i provjerljivi, što je u konkretnom slučaju ispunjeno. Nadalje, naručitelj smatra neosnovanim navod da je trebao navesti točan broj dnevnih korisnika RIS sustava, budući da taj podatak nije nužan za izradu usporedive ponude niti za razumijevanje predmeta nabave. Ističe da se radi o referentnom podatku koji nije predmet ugovaranja niti služi za obračun usluga, već isključivo kao indikator razine složenosti sustava i iskustva koje se traži od stručnjaka. Ujedno navodi da je žalitelj, ako je smatrao taj podatak relevantnim, mogao zatražiti pojašnjenje dokumentacije, što nije učinio. Stoga samo nenavođenje točnog broja korisnika ne dovodi u pitanje jasnoću i razumljivost dokumentacije o nabavi.

Ocjenjujući žalbeni navod ovo tijelo polazi od utvrđenog činjeničnog stanja te odredbi članka 200. stavak 1. ZJN 2016.

U odnosu na predmetni žalbeni navod, ovo tijelo ukazuje da je u okviru ocjene prvog i drugog žalbenog navoda već utvrđeno da osporeni uvjeti tehničke i stručne sposobnosti za stručnjake S1, S2, S3, S5 i S6 pa time i kriterij za odabir ekonomski najpovoljnije ponude nisu protivni ZJN 2016.

Prema ocjeni ovog tijela okolnost da sama tehnička specifikacija RIS sustava koji je predmet održavanja koje se nabavlja u okviru ovog postupka ne sadrži izrijekom navedene funkcionalnosti iskustvo na implementaciji kojih se u konkretnom slučaju boduje kao kriterij ekonomski najpovoljnije ponude sama po sebi ne dovodi u pitanje jasnoću dokumentacije o nabavi, budući da iz njezine cjelokupne strukture i sadržaja proizlazi jasna razdioba između opisa predmeta nabave, uvjeta sposobnosti i kriterija za odabir ponude.

U odnosu na navode žalitelja koji osporavaju jasnoću pojma „broj dnevnih korisnika“, prihvaća se argumentacija naručitelja da se radi o standardnom pojmu u području informacijskih sustava koji služi za procjenu opsega, opterećenja i složenosti sustava te razlikovanje iskustva na manjim i zatvorenim sustavima od iskustva na sustavima s većim brojem korisnika. Isto je tako prihvaćena i njegova argumentacija da je način dokazivanja tog podatka objektivan i provjerljiv te da se može dokazivati kroz projektne reference, tehničke opise, potvrde naručitelja i drugu relevantnu dokumentaciju.

Naručitelj je, sukladno dokumentaciji o nabavi, propisao minimalne vrijednosti broja dnevnih korisnika za pojedine projekte i aktivnosti koje se vrednuju kod stručnjaka. Prihvaća se i argumentacija naručitelja da se navedeni podatak može dokazivati različitim objektivno provjerljivim dokaznim sredstvima, uključujući projektne reference, tehničke opise, potvrde naručitelja i drugu relevantnu dokumentaciju, budući da ZJN 2016 ne propisuje obvezu određivanja jedinstvene metodologije dokazivanja svakog pojedinog tehničkog podatka, već je dostatno da je kriterij formuliran na način koji je objektivan, razumljiv i provjerljiv, što je u konkretnom slučaju ispunjeno.

Slijedom svega navedenog, ocjenjuje se da žalitelj nije dokazao da bi dokumentacija o nabavi u osporenom dijelu bila nejasna, neprecizna odnosno sastavljena protivno članku 200. stavku 1. ZJN 2016, niti da bi onemogućavala podnošenje usporedivih ponuda, radi čega se predmetni žalbeni navod ocjenjuje neosnovanim.

Žalitelj ujedno navodi da su uvjeti tehničke i stručne sposobnosti te kriteriji za odabir ponude definirani protivno člancima 268., 285. i 200. ZJN 2016. Ističe da je naručitelj u dokumentaciji o nabavi, pod točkom 3.4. „Kriteriji za odabir ponuda“ te u dokumentu „Kriterij za odabir ekonomski najpovoljnije ponude“, odredio kriterij kvalitete i bodovanje za specifično iskustvo stručnjaka S1 i S2. Nadalje navodi da se istim iskustvom (referencom) stručnjaka ocjenjuje i tehnička i stručna sposobnost i kriterij za odabir ponude, što, prema njegovom mišljenju, dovodi do preklapanja dviju faza ocjene. Kao primjer navodi prvi kriterij kvalitete za stručnjaka S1 kojim je propisano da će „za svaki završeni projekt implementacije WAF rješenja za zaštitu web aplikacija na softverima za minimalno 1000 dnevnih korisnika naručitelj umanjiti cijenu ponude za 4.000,00 EUR po projektu do najviše 20.000,00 EUR za 5 projekata“. Žalitelj ističe da je navedeni kriterij u odnosu na traženo iskustvo istovjetan prvom uvjetu tehničke i stručne sposobnosti za stručnjaka S1 prema kojem „stručnjak mora imati iskustvo u minimalno jednom završenom projektu implementacije WAF rješenja za zaštitu web aplikacija u svojstvu stručnjaka za sigurnost informacijskih sustava na softverima za minimalno 1000 dnevnih korisnika“. Obzirom da naručitelj kod tog kriterija za odabir ponude koristi izričaj „za svaki završeni projekt implementacije“, iz toga proizlazi da će bodove (umanjenje cijene) za kriterij specifičnog iskustva dodjeljivati i za prvu referencu koju ocjenjuje kao uvjet sposobnosti.

Žalitelj ističe da je člankom 268. stavkom 8. ZJN 2016 propisano da se tehnička i stručna sposobnost može dokazivati kroz obrazovne i stručne kvalifikacije pružatelja usluge ili izvođača radova ili njihova rukovodećeg osoblja, uz uvjet da se iste ne ocjenjuju u okviru kriterija za odabir ponude. Iako je naručitelj uvjete za stručnjake definirao kroz tehničke stručnjake, žalitelj smatra da se u bitnome radi o stručnim kvalifikacijama pružatelja usluge, zbog čega se ista (prva) referenca ne može istodobno koristiti i kao uvjet tehničke i stručne sposobnosti i kao kriterij za odabir ponude. Nadalje navodi da navedeno u dokumentaciji nije jasno i precizno određeno, uslijed čega gospodarski subjekti nisu u mogućnosti nedvojbeno utvrditi koliko referenci moraju navesti kako bi ostvarili određeni broj bodova (umanjenje cijene), što dovodi u pitanje sukladnost dokumentacije s člankom 200. stavkom 1. ZJN 2016. Također upućuje na članak 285. stavak 3. ZJN 2016, prema kojem je naručitelj dužan odrediti kriterije za odabir ponude na način koji omogućava učinkovit pregled i ocjenu ponuda, pri čemu, prema žalitelju, nije jasno kako će se osigurati takav pregled i ocjena ako se ne razgraniči hoće li se i na koji način bodovati i prva referenca koja istodobno

predstavlja uvjet sposobnosti. Žalitelj se pritom poziva i na praksu Suda Europske unije predmet C-532/06 Lianakis.

Naručitelj u odgovoru na žalbu osporava navode žalitelja te ističe da je u okviru uvjeta tehničke i stručne sposobnosti propisao minimalni zahtjev da stručnjaci moraju imati iskustvo u najmanje jednom završenom projektu. Nadalje, pojašnjava da je u kriterijima za odabir ekonomski najpovoljnije ponude jasno određeno da će se ponudama u kojima se nudi iskustvo stručnjaka iznad minimalno propisanog standarda umanjivati ponuđena cijena, pri čemu se takvo umanjenje odnosi na iskustvo stečeno u drugom i svakom sljedećem projektu, budući da prvi projekt predstavlja ispunjenje minimalnog uvjeta tehničke i stručne sposobnosti.

Ocjenjujući žalbeni navod, ovo tijelo polazi od utvrđenog činjeničnog stanja te odredbe članka 200. stavka 1. ZJN 2016.

Uzimajući u obzir činjenično stanje utvrđeno prilikom ocjene prvog i drugog žalbenog navoda, kao i sadržaj dokumentacije o nabavi, utvrđeno je da je u točki 5.2.2.4. dokumentacije o nabavi, u okviru uvjeta tehničke i stručne sposobnosti, za stručnjake S1 i S2 propisano minimalno iskustvo koje stručnjaci moraju posjedovati za izvršenje predmeta nabave, pri čemu je za pojedina područja iskustva određeno da stručnjak mora imati iskustvo u najmanje jednom završenom projektu. Nadalje, u dijelu dokumentacije koji se odnosi na kriterije za odabir ekonomski najpovoljnije ponude propisano je bodovanje dodatnog iskustva stručnjaka kroz broj završenih projekata iznad minimalno zahtijevane razine iskustva.

Iz navedenog proizlazi da dokumentacija o nabavi razlikuje minimalne uvjete tehničke i stručne sposobnosti, kojima se utvrđuje sposobnost gospodarskog subjekta za izvršenje ugovora, od kriterija za odabir ekonomski najpovoljnije ponude, kojima se vrednuje dodatna kvaliteta i razina iskustva stručnjaka radi međusobnog rangiranja prihvatljivih ponuda.

Slijedom navedenoga, prema ocjeni ovog tijela, iz dokumentacije o nabavi na jasan i nedvojben način proizlazi razgraničenje između iskustva koje se zahtijeva kao minimalni uvjet sposobnosti i iskustva koje se vrednuje u okviru kriterija za odabir ekonomski najpovoljnije ponude, zbog čega nisu osnovani žalbeni navodi da nije jasno hoće li se i na koji način bodovati referenca kojom se dokazuje ispunjenje minimalnog uvjeta sposobnosti.

Nadalje, žalitelj se neosnovano poziva na presudu Suda Europske unije u predmetu C-532/06 Lianakis, budući da se u konkretnom slučaju ne radi o situaciji u kojoj se isto iskustvo ili iste kvalifikacije istodobno koriste kao uvjet sposobnosti i kao kriterij za odabir ponude, već je dokumentacijom o nabavi uspostavljena razlika između minimalno zahtijevane razine iskustva i dodatnog iskustva koje se vrednuje radi rangiranja ponuda.

Slijedom svega navedenog, ovo tijelo ocjenjuje da je dokumentacija o nabavi u osporenom dijelu jasna, precizna, razumljiva i nedvojbena te da omogućuje podnošenje usporedivih ponuda, zbog čega žalbeni navod nije osnovan.

Postupajući po službenoj dužnosti temeljem članka 404. ZJN 2016, a u odnosu na osobito bitne povrede postupka javne nabave iz članka 404. stavka 2. toga Zakona, ovo državno tijelo nije utvrdilo postojanje osobito bitnih povreda.

Slijedom navedenog, temeljem članka 425. stavka 1. točke 4. ZJN 2016, odlučeno je kao u točki 1. izreke ovog rješenja.

Žalitelj je postavio zahtjev za naknadom troškova žalbenog postupka u ukupnom iznosu od 3.120,00 eur. Sukladno odredbi članka 431. stavka 4. ZJN 2016 u slučaju obijanja žalbe žalitelj nema pravo na naknadu troškova žalbenog postupka. Slijedom navedenog odlučeno je kao u točki 2. izreke rješenja.

UPUTA O PRAVNOM LIJEKU

Protiv ovog rješenja nije dopuštena žalba, ali se može pokrenuti upravni spor pred Visokim upravnim sudom Republike Hrvatske u roku od 30 dana od isteka osmog dana od dana javne objave rješenja na internetskim stranicama Državne komisije za kontrolu postupaka javne nabave. Tužba se predaje neposredno u pisanom obliku, usmeno na zapisnik ili se šalje poštom, odnosno dostavlja u elektroničkom obliku putem informacijskog sustava.

PREDSJEDNICA

Maja Kuhar

MAJA KUHAR
HR-86166416407

Elektronički potpisano: 19.06.2026T11:41:36 (UTC:2026-06-19T09:41:36Z)
Provjera: https://epotpis.rdd.hr/provjera
Broj zapisa: b18edaee-05f7-4749-9196-0e3ec2050bf9