Prilog III

PROJEKTNI ZADATAK

NIS2 Direktiva: Analiza usklađenosti te akcijski plan provedbe usklađivanja sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti

Osijek, travanj 2025.

Sadržaj

1. Uvod

Sigurnost kritične infrastrukture ima temeljnu važnost za očuvanje stabilnosti država i funkcioniranje društva. Među sektorima koji čine ključnu infrastrukturu ističu se energetika, promet, zdravstvo i digitalna infrastruktura. Unutar sektora zdravstva, institucije poput referentnih laboratorija zauzimaju istaknuto mjesto, omogućujući zaštitu javnog zdravlja, nadzor sigurnosti hrane i učinkovit odgovor na biološke rizike.

Uzimajući u obzir sve veću izloženost informacijskih sustava prijetnjama iz kibernetičkog prostora, Europska unija donijela je Direktivu o mrežnoj i informacijskoj sigurnosti (NIS2). Ova direktiva proširuje zahtjeve prethodnog regulatornog okvira te širi krug subjekata koji su obvezni provoditi mjere za podizanje razine kibernetičke sigurnosti, uključujući i referentne laboratorije te institucije iz sektora zdravstva.

Direktiva NIS2 stupila je na snagu krajem 2022. godine, a u pravni sustav Republike Hrvatske prenesena je kroz **Zakon o kibernetičkoj sigurnosti** (NN 14/2024), koji se primjenjuje od 15. veljače 2024. godine, te dodatno operacionalizirana **Uredbom o kibernetičkoj sigurnosti** (NN 135/2024), koja se primjenjuje od 29. studenog 2024. godine.

S obzirom na značaj referentnih laboratorija i institucija koje pružaju ključne usluge za javno zdravstvo, posebno u sustavu sigurnosti hrane i biološke sigurnosti, subjekti poput Hrvatske agencije za poljoprivredu i hranu obvezni su provoditi mjere za zaštitu svojih informacijskih i komunikacijskih sustava te sustavno upravljati rizicima vezanim uz kibernetičku sigurnost.

Iz obveza koje proizlaze iz Direktive o mrežnoj i informacijskoj sigurnosti (NIS2), Zakona o kibernetičkoj sigurnosti i Uredbe o kibernetičkoj sigurnosti, izdvajaju se sljedeći zahtjevi:

- uvođenje i održavanje tehničkih i organizacijskih mjera za sigurnost mrežnih i informacijskih sustava
- redovita procjena kibernetičkih rizika i implementacija odgovarajućih mjera zaštite
- praćenje sigurnosnih događaja i prijavljivanje incidenata u propisanim rokovima
- izrada i redovito ažuriranje planova za kontinuitet poslovanja i krizno upravljanje u slučaju kibernetičkog incidenta.

Neusklađenost s navedenim zakonodavnim okvirom može dovesti do značajnih sankcija, uključujući:

- novčane kazne do 10 milijuna eura ili do 2 % godišnjeg ukupnog prihoda za ključne subjekte
- prekršajne kazne za odgovorne osobe unutar organizacijske strukture.

Kako bi ispunila zakonske zahtjeve i unaprijedila razinu kibernetičke otpornosti, Hrvatska agencija za poljoprivredu i hranu pokreće postupak izrade analize usklađenosti s Direktivom o mrežnoj i informacijskoj sigurnosti (NIS2) te nacionalnim regulatornim aktima, Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti, uključujući razvoj akcijskog plana kojim će se definirati konkretni koraci za zaštitu informacijske infrastrukture i očuvanje kontinuiteta ključnih funkcija unutar sektora zdravstva.

2. Predmet nabave

Učinkovita provedba Zakona o kibernetičkoj sigurnosti i Uredbe o kibernetičkoj sigurnosti nije samo zakonska obveza značajno doprinosi zaštiti kritične zdravstvene infrastrukture i jačanju otpornosti na sve složenije kibernetičke prijetnje koje mogu ugroziti sigurnost laboratorijskih sustava, vjerodostojnost analitičkih podataka i integritet informacijskih procesa povezanih s javnim zdravljem. Pravodobno usklađivanje omogućit će Naručitelju ne samo ispunjavanje regulatornih zahtjeva i izbjegavanje sankcija, već i jačanje povjerenja korisnika i partnera te osiguranje pouzdanog i sigurnog funkcioniranja digitalnih sustava podrške poslovnim i stručnim procesima.

Ponuditelj će pružiti stručnu podršku Naručitelju u pripremi i dostavi potrebnih podataka i procjena za potrebe nacionalne procjene kibernetičkih sigurnosnih rizika, koju provodi nadležno državno tijelo za kibernetičku sigurnost u okviru prvog postupka kategorizacije subjekata, sukladno Uredbi o kibernetičkoj sigurnosti.

Predmet ove nabave je pružanje usluge izrade analize, odnosno samoprocjene usklađenosti sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti, te izrada akcijskog plana usklađivanja koji obuhvaća sustave informacijske tehnologije (IT), uključujući sustave za upravljanje laboratorijskim analizama, digitalno izvještavanje, sigurnosni nadzor laboratorijskih procesa te komunikacijske protokole relevantne za rad referentnih laboratorija i zdravstvenih institucija.Analiza i plan će biti izrađeni u skladu s relevantnim standardima i smjernicama, uključujući:

- ISO 27001 (upravljanje informacijskom i kibernetičkom sigurnosti)
- ISO 22301 (upravljanje kontinuitetom poslovanja)
- ENISA smjernice i sektorske preporuke za upravljanje rizicima

Ponuditelj je obvezan isporučiti sljedeće usluge:

1. **Analizu (samoprocjenu) usklađenosti sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti**
2. **Akcijski plan za usklađenje s propisima i sigurnosnim standardima**
3. **Edukaciju o regulatornim obvezama i specifičnim zahtjevima za sektor**

3. Izazovi naručitelja vezani uz kibernetičku sigurnost

Naručitelj je prepoznao ključne izazove povezane s kibernetičkom sigurnošću i usklađivanjem s propisima Zakona o kibernetičkoj sigurnosti, Uredbe o kibernetičkoj sigurnosti, koji su od posebnog značaja za sektor zdravstva i referentnih laboratorija:

1. Laboratorijski informacijski sustavi, baze podataka o uzorcima, rezultati ispitivanja i dijagnostičke platforme često su razvijeni u razdoblju kada kibernetička sigurnost nije bila primarni fokus. Potrebno je identificirati ranjivosti i slabosti tih sustava kako bi se omogućila njihova usklađenost sa suvremenim sigurnosnim zahtjevima i zaštitila točnost i integritet podataka.
2. Pojedini laboratoriji, ispitna postrojenja i skladišta uzoraka nalaze se na udaljenim ili manje nadziranima lokacijama, što ih čini osjetljivima na fizičke prijetnje, neovlašteni pristup ili sabotaže koje mogu ugroziti sigurnost uzoraka, rezultata i infrastrukture.
3. Zaposlenici, vanjski suradnici ili izvođači koji imaju pristup laboratorijskim informacijskim sustavima i bazama podataka predstavljaju potencijalni izvor nenamjernih grešaka ili namjernih

sigurnosnih incidenata. Prepoznavanje, nadzor i pravilno upravljanje ovim rizicima ključno je za očuvanje povjerljivosti i integriteta podataka.

4. Laboratoriji često surađuju s vanjskim IT servisima, pružateljima analitičkih platformi ili dobavljačima softvera koji ostvaruju pristup kritičnim informacijskim sustavima. Potrebno je provesti stroge kontrole pristupa, provjeru sigurnosnih mjera kod trećih strana i upravljanje rizicima dobavljača.
5. Laboratorijski informacijski sustavi (npr. sustavi za obradu nalaza, sustavi za praćenje kvalitete, elektroničke baze podataka o uzorcima) ključni su za svakodnevni rad laboratorija i osiguranje vjerodostojnosti rezultata. Regulativa zahtijeva uspostavu strukturiranog procesa upravljanja rizicima za ove sustave, čime se štiti kontinuitet laboratorijskih usluga i povećava otpornost na kibernetičke prijetnje koje bi mogle dovesti do prekida rada ili kompromitacije podataka.

4. Analiza usklađenosti sa ZKS/UKS/NIS2

Za učinkovitu provedbu aktivnosti usklađivanja sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti, Ponuditelj je obvezan provesti sljedeće korake, prilagođene poslovanju referentnog laboratorija i institucije iz sektora zdravstva:

- **Analiza interne dokumentacije** – potrebno je pregledati sve interne akte, pravilnike i politike Naručitelja koji se odnose na upravljanje informacijskom sigurnošću, zaštitu laboratorijskih podataka, kontinuitet rada laboratorija i odgovor na incidente.
- **Identifikacija ključnih poslovnih procesa** – definirati kritične laboratorijske i administrativne procese čije neometano funkcioniranje osigurava provedbu ispitivanja, verifikaciju rezultata, sigurnost hrane te javnozdravstveni nadzor. Provodi se sveobuhvatna analiza utjecaja na poslovanje (Business Impact Analysis – BIA).
- **Procjena sigurnosti fizičkih i digitalnih lokacija** – provjeriti postojeće sigurnosne mjere na laboratorijskim lokacijama, centrima za obradu podataka, uzorkovnim mjestima i skladištima uzoraka, uključujući zaštitu od fizičkih i digitalnih prijetnji.
- **Analiza ugovora s trećim stranama** – pregledati ugovorne odnose s vanjskim dobavljačima IT usluga, održavanja laboratorijskih sustava i digitalne infrastrukture, s ciljem procjene njihove usklađenosti s kibernetičkim sigurnosnim zahtjevima te otpornosti na incidente.
- **Procjena sigurnosti dobavljačkog lanca** – utvrditi potrebu za nadzorom ili revizijom trećih strana koje imaju pristup kritičnim laboratorijskim informacijskim sustavima, u skladu s načelima i obvezama iz Zakona o kibernetičkoj sigurnosti, Uredbe o kibernetičkoj sigurnosti i Direktive o mrežnoj i informacijskoj sigurnosti (NIS2).
- **Analiza sektorskih specifičnosti** – prepoznati specifične izazove zdravstvenog sektora poput osjetljivosti podataka o zdravlju, zakonskih obveza zaštite podataka, potrebe za očuvanjem kontinuiteta laboratorijskih analiza te suradnje s nacionalnim i međunarodnim tijelima.
- **Procjena prijetnji ključnim uslugama** – evidentirati moguće scenarije koji bi mogli ugroziti ključne laboratorijske funkcije, digitalno izvještavanje i sigurnosne protokole te procijeniti njihov potencijalni utjecaj na stabilnost usluga.
- **Analiza postojećih planova i procedura** – identificirati i procijeniti postojeće dokumente relevantne za izradu Plana kontinuiteta poslovanja (Business Continuity Plan – BCP) i Plana oporavka od ugroza (Disaster Recovery Plan – DRP), posebno usmjerene na rad laboratorijskih i IT sustava.

Ishod ove aktivnosti je Izvješće o provedenoj analizi spremnosti sustava za očuvanje kontinuiteta

poslovanja i otpornosti kritičnih laboratorijskih usluga. Izvješće će sadržavati nalaze, procjene postojećeg stanja te preporuke za unaprjeđenje sigurnosti, izrađene u skladu s propisima Zakona o kibernetičkoj sigurnosti, Uredbe o kibernetičkoj sigurnosti i relevantnih standardia i smjernica.

Nakon dostave, Naručitelj ima rok od 15 dana za dostavljanje primjedbi, zahtjeva za dodatna objašnjenja ili dopuna. Ako Naručitelj u tom roku ne dostavi očitovanje, smatrat će se da je sadržaj Izvješća prihvaćen. U slučaju dostavljenih zahtjeva, Ponuditelj je dužan izvršiti potrebne izmjene u roku od 15 dana ili u drugom dogovorenom roku.

5. Izrada Akcijskog Plana USKLAĐIVANJA

Nakon izrade Izvješća o provedenoj analizi spremnosti informacijskih i laboratorijskih sustava za osiguranje kontinuiteta poslovanja i otpornosti ključnih usluga, Izvršitelj je obvezan pripremiti Prijedlog akcijskog plana za usklađivanje sa Zakonom o kibernetičkoj sigurnosti i Uredbom o kibernetičkoj sigurnosti.

Akcijski plan će biti izrađen temeljem sveobuhvatne analize identificiranih nalaza, te će sadržavati konkretne mjere, aktivnosti, resurse i odgovornosti potrebne za jačanje kibernetičke sigurnosti i usklađivanje sustava Naručitelja s propisanim zahtjevima. Plan će uključivati jasan vremenski okvir provedbe aktivnosti te prioritizaciju mjera prema razini identificiranog rizika i utjecaju na kontinuitet laboratorijskih i administrativnih funkcija.

Aktivnosti definirane Akcijskim planom bit će usmjerene na minimiziranje rizika koji bi mogli ugroziti obradu laboratorijskih uzoraka, upravljanje zdravstveno relevantnim podacima, sigurnost informacijskih sustava te pouzdanost usluga povezanih sa zaštitom zdravlja i sigurnošću hrane.

Prijedlog Akcijskog plana bit će dostavljen Naručitelju na pregled. Naručitelj ima rok od 15 dana za dostavljanje komentara, prijedloga izmjena ili zahtjeva za dodatnim pojašnjenjima. U slučaju zaprimanja očitovanja, Izvršitelj je dužan prilagoditi Akcijski plan u skladu s dostavljenim zahtjevima u roku od 15 dana, ili u drugom roku ako ga stranke posebno dogovore.

Ukoliko Naručitelj ne dostavi očitovanje u predviđenom roku, smatrat će se da je Prijedlog Akcijskog plana prihvaćen, a aktivnost završena.

Važno je napomenuti da Prijedlog Akcijskog plana ima karakter smjernica i preporuka te ne obvezuje Naručitelja na implementaciju predloženih mjera u zadanom opsegu ili vremenskom okviru, već služi kao temelj za planiranje i provedbu budućih koraka u jačanju kibernetičke sigurnosti. Ako Naručitelj ne dostavi očitovanje u roku od 15 dana, smatra se da je suglasan s prijedlogom, te se aktivnost smatra izvršenom. Važno je napomenuti da Prijedlog Akcijskog plana ne predstavlja obvezu Naručitelja za implementaciju u zadanom opsegu ili rokovima, već služi kao smjernica za daljnje korake u procesu usklađivanja.

6. Edukacija o Regulativi i Specifičnim Obvezama u Zahtjevima Usklađivanja

Izvršitelj je obvezan organizirati ciljanu edukaciju za najviše 30 sudionika iz redova višeg, srednjeg i operativnog menadžmenta Naručitelja, na lokaciji koju odredi Naručitelj. Svi pripadajući troškovi organizacije i izvođenja edukacije s Izvršiteljeve strane uključeni su u ukupnu ugovorenu cijenu usluge.

Edukacija ima za cilj podići razinu razumijevanja i spremnosti institucije za učinkovito usklađivanje s propisima iz područja kibernetičke sigurnosti, posebno u kontekstu specifičnih izazova s kojima se suočavaju referentni laboratoriji, znanstvene jedinice i službe za sigurnost hrane.

Tijekom edukacije, sudionici će biti upoznati sa sljedećim ključnim temama:

- **Zakonodavni okvir** – predstavljanje važećih regulatornih zahtjeva, uključujući Direktivu o mrežnoj i informacijskoj sigurnosti (NIS2), Zakon o kibernetičkoj sigurnosti i Uredbu o kibernetičkoj sigurnosti, s naglaskom na njihove primjene u zdravstvenim, laboratorijskim i kontrolnim institucijama.
- **Rizici i slabosti identificirani tijekom analize sustava** – sudionici će biti upoznati s nalazima iz prethodno izrađenog Izvješća o spremnosti sustava, kao i s preporukama za unaprjeđenje otpornosti i sigurnosti, uz naglasak na prioritetne ranjivosti koje mogu utjecati na pouzdanost laboratorijskih podataka i kontinuitet ključnih usluga.
- **Obveze po razinama odgovornosti** – razjašnjavanje uloga različitih organizacijskih razina u procesu provedbe mjera za smanjenje rizika i usklađivanje s regulatornim zahtjevima, uključujući i odgovornost za prijenos znanja i svijesti o sigurnosti prema operativnom osoblju.
- **Sankcije i rokovi** – prikaz mogućih posljedica neusklađenosti s propisima, uključujući novčane i organizacijske sankcije, te pregled zakonski propisanih rokova za otklanjanje utvrđenih nedostataka.

Aktivnost edukacije smatra se uspješno izvršenom po završetku jednodnevne obuke svih planiranih sudionika, čime se osigurava osnovna razina razumijevanja i kapaciteta potrebna za daljnju provedbu mjera kibernetičke sigurnosti u djelatnostima laboratorijskih ispitivanja, kontrole i zaštite zdravlja u skladu s važećim zakonodavstvom i strukovnim smjernicama.

7. OBVEZE NARUČITELJA

Za uspješnu i pravovremenu provedbu projektnih aktivnosti povezanih s usklađivanjem s Direktivom o mrežnoj i informacijskoj sigurnosti (NIS2), Zakonom o kibernetičkoj sigurnosti te Uredbom o kibernetičkoj sigurnosti, ključno je osigurati aktivno i strukturirano sudjelovanje Naručitelja. Uspješnost projekta ne ovisi samo o kvaliteti isporuke Izvršitelja, već i o kvalitetnoj suradnji i dostupnosti resursa unutar same organizacije.

Naručitelj se, u tom kontekstu, obvezuje imenovati odgovornu osobu koja će imati ovlast i odgovornost za koordinaciju svih aktivnosti vezanih uz projekt. Ta osoba djelovat će kao središnja kontakt točka prema Izvršitelju, osiguravajući pravovremenu razmjenu informacija, dostupnost dokumentacije te organizaciju sudjelovanja relevantnog osoblja. Kroz ovu funkciju osigurava se dosljednost u komunikaciji i učinkovita implementacija planiranih mjera, čime se izbjegavaju nesporazumi i nepotrebna kašnjenja.

Naručitelj će omogućiti pristup svim relevantnim dokumentima koji su ključni za analizu trenutnog stanja i izradu akcijskog plana. To uključuje interne politike i procedure koje se odnose na upravljanje informacijskom sigurnošću, zaštitu laboratorijskih podataka, obradu uzoraka, praćenje neusklađenosti, kao i dokumentaciju o postojećim tehničkim i organizacijskim mjerama. Otvoren i pravodoban uvid u ove informacije nužan je kako bi Izvršitelj mogao izraditi preciznu procjenu postojećih rizika te ponuditi mjere usklađene sa stvarnim operativnim potrebama laboratorijske i zdravstvene djelatnosti.

Za vrijeme provedbe projekta, Naručitelj će osigurati potrebne ljudske, organizacijske i tehničke resurse. To podrazumijeva angažman stručnog osoblja iz pojedinih odjela (npr. informacijska sigurnost, IT podrška, laboratorijska obrada, upravljanje kvalitetom), ali i dostupnost tehničke infrastrukture koja je predmet

analize. Time se stvara preduvjet za točnu i detaljnu procjenu ranjivosti, kao i za izradu konkretnih preporuka za jačanje otpornosti organizacije na kibernetičke prijetnje.

8. OBVEZE IZVRŠITELJA

Izvršitelj preuzima obvezu aktivnog, profesionalnog i kontinuiranog sudjelovanja u provedbi ugovora, s punim razumijevanjem važnosti projekta za sigurnost i otpornost Naručiteljevih informacijskih, laboratorijskih i zdravstvenih sustava. Pružanje usluge temeljit će se na načelima povjerenja, stručnosti i zakonodavne usklađenosti, s posebnim naglaskom na interese i specifične potrebe institucije koja djeluje u javnozdravstvenom i znanstveno-analitičkom kontekstu.

U cilju ispunjavanja svih obveza, Izvršitelj se obvezuje angažirati stručnjake s dokazanim znanjem i iskustvom u području informacijske sigurnosti, upravljanja rizicima, zaštite osobnih i osjetljivih podataka te implementacije regulatornih okvira kao što su Direktiva o mrežnoj i informacijskoj sigurnosti (NIS2), Zakon o kibernetičkoj sigurnosti i Uredba o kibernetičkoj sigurnosti. Stručni tim mora posjedovati relevantne certifikate i sposobnost rada u kompleksnim zdravstvenim i laboratorijskim sustavima gdje točnost, povjerljivost i otpornost predstavljaju osnovu svakodnevnog rada.

Provedba aktivnosti predviđa različite oblike suradnje, uključujući radne sastanke s predstavnicima Naručitelja, samostalnu analitičku obradu od strane Izvršitelja, kao i zajednički rad timova obje strane u fazama koje zahtijevaju funkcionalno i tehničko usklađivanje. Kroz trajnu koordinaciju osigurat će se jasno praćenje napretka, praćenje identificiranih rizika i pravovremeno reagiranje u skladu s utvrđenim prioritetima.

Dio aktivnosti Izvršitelja može se odvijati i na fizičkim lokacijama Naručitelja, kao što su laboratoriji, uredske jedinice, podatkovni centri i drugi objekti koji podliježu analizi, ali i u prostorima Izvršitelja, ovisno o vrsti zadatka. Također se predviđa mogućnost korištenja digitalnih kanala i alata za potrebe daljinske podrške, virtualne edukacije ili elektroničke razmjene podataka, uz poštivanje najviših standarda informacijske sigurnosti.

Sve informacije do kojih Izvršitelj dođe tijekom provedbe ugovora smatrat će se poslovnom i profesionalnom tajnom. One se ne smiju priopćavati trećim stranama bez prethodne pisane suglasnosti obje ugovorne strane. To se posebno odnosi na podatke koji se tiču sigurnosnih procedura, laboratorijskih nalaza, zdravstvenih nadzora i internih operativnih procedura, čije neovlašteno otkrivanje može ugroziti sigurnost, ugled ili zakonsku usklađenost Naručitelja.

Na taj način, Izvršitelj osigurava visoku razinu profesionalne odgovornosti i doprinosi stvaranju povjerenja nužnog za uspješno provođenje aktivnosti u osjetljivom sektoru zaštite zdravlja, laboratorijskih analiza i sigurnosti hrane.

9. NUĐENJE PREDMETA NABAVE I KOLIČINE

Ponuditelj je dužan nuditi isključivo cjelokupan predmet nabave sukladno troškovniku, uključujući sve specifične usluge i resurse potrebne za usklađivanje s regulativom i kibernetičkim standardima za predmetni sektor.

10. MJESTO I NAČIN PRUŽANJA PREDMETA NABAVE

Mjesto pružanja usluge, odnosno izvršenja ugovora, bit će lokacije sjedišta Naručitelja i Izvršitelja, uz

mogućnost izvršenja usluga putem *online* kanala za daljinsku podršku, obuku i izvještavanje.

11. ROK TRAJANJA UGOVORA

Ugovor stupa na snagu danom potpisa obje ugovorne strane, a rok trajanja Ugovora je 8 (osam) mjeseci. Rok trajanja Ugovora može se produžiti ukoliko dođe do promjena u zakonskoj regulativi koja utječe na predmet nabave ili drugih opravdanih razloga koji nastanu tijekom trajanja Ugovora.

Izvršitelj je obvezan predmet nabave izvršavati kontinuirano, u skladu s odredbama ovog projektnog zadatka, posebno s naglaskom na pravovremeno ispunjavanje svih sigurnosnih zahtjeva i zakonskih obveza. Izvršitelj se obvezuje izvršiti sve aktivnosti definirane troškovnikom i usklađene s regulativama u krajnjem roku od 8 (osam) mjeseci od potpisa Ugovora.

Izvršitelj je u obvezi odmah po potpisu Ugovora pokrenuti projekt inicijalnim sastankom, na kojem će sudjelovati ključni dionici, kako bi se identificirali svi relevantni dionici, uspostavio projektni tim, te usuglasio pristup provedbi projekta i definirao vremenski projektni plan.

Uredno izvršenje predmeta nabave potvrđuje se odgovarajućim zapisnikom o isporuci, koji mora biti ovjeren od strane koordinatora obje ugovorne strane.

12. KRITERIJI ZA ODABIR GOSPODARSKOG SUBJEKTA (UVJETI SPOSOBNOSTI)

Gospodarski subjekt mora dokazati sposobnost kako slijedi:

A. Sposobnost za obavljanje profesionalne djelatnosti

Kako bi dokazao sposobnost za obavljanje profesionalne djelatnosti, ponuditelj je dužan dokazati upis u sudski, obrtni, strukovni ili drugi odgovarajući registar u državi njegova poslovnog nastana.

Kao dokaz sposobnosti za obavljanje profesionalne djelatnosti, Naručitelj će prihvatiti:

Izvadak iz sudskog, obrtnog, strukovnog ili drugog odgovarajućeg registra koji se vodi u državi članici njegova poslovnog nastana. Izvadak ne smije biti stariji od 3 mjeseca računajući od dana slanja ovog Poziva.

B. Tehnička i stručna sposobnost

B.1. Popis usluga

Naručitelj određuje uvjete tehničke i stručne sposobnosti kojima se osigurava da ponuditelj ima potrebne ljudske i tehničke resurse te iskustvo potrebno za izvršenje ugovora o jednostavnoj nabavi na odgovarajućoj razini kvalitete, što se dokazuje odgovarajućim referencijama iz prije izvršenih ugovora.

Tehnička i stručna sposobnost iz ove točke dokazuje se popisom glavnih usluga pruženih u godini u kojoj je započeo postupak jednostavne nabave i tijekom četiri godine koje prethode toj godini. Smatra se da je uvjet tehničke i stručne sposobnosti vezan uz predmet nabave ako su usluge iste ili slične predmetu nabave.

Dokaz iz ove točke mora biti razmjeran predmetu nabave, te ponuditelj mora dokazati da je u godini u

kojoj je započeo postupak jednostavne nabave i tijekom četiri godine koje prethode toj godini pružio:

- Najmanje jednu (1), a najviše tri (3) glavne usluge iste ili slične predmetu nabave čija je vrijednost najmanje jednaka 20.000,00 EUR-a bez PDV-a, pri čemu minimalno jedna (1) od njih mora biti iz sektora zdravstvenih odnosno laboratorijskih usluga.

Kao dokaz tehničke i stručne sposobnosti iz ove točke, ponuditelj u ponudi dostavlja:

- Popis glavnih usluga istih ili sličnih predmetu nabave, pruženih u godini u kojoj je započeo postupak nabave i tijekom četiri godine koje prethode toj godini.

Popis sadržava:

- naziv druge ugovorne strane (Naručitelja)
- naziv pružatelja usluge
- predmet i opis pružene usluge iz kojeg će naručitelj moći nedvojbeno utvrditi ispunjava li gospodarski subjekt traženi uvjet tehničke i stručne sposobnosti
- vrijednost pružene usluge
- razdoblje pružanja usluge.

B.2. Tehnički stručnjaci

Popis tehničkih stručnjaka i traženi certifikati

U svrhu osiguranja kvalitetnog izvršenja usluga, a zbog kompleksnosti sustava Naručitelja i traženog modela upravljanja, gospodarski subjekt mora dokazati da na raspolaganju ima dovoljno certificiranih i stručnih osoba koje mogu kvalitetno pružiti podršku i u slučajevima potrebe za povećanim angažmanom, a najmanje:

VODEĆI STRUČNJAK ZA REVIZIJU KIBERNETIČKE SIGURNOSTI I OTPORNOSTI – VODITELJ PROJEKTA – 1 izvršitelja

U okviru ovog uvjeta tehničke i stručne sposobnosti, svi nominirani stručnjak iz predmetne grupe mora ispunjavati sve niže navedene uvjete u pogledu kvalifikacija i vještina te općenitog stručnog iskustva.

S obzirom da se radi o kibernetičkoj sigurnosti i otpornosti odnosno kontinuitetu poslovanja te regulatornim specifičnostima, vodeći stručnjak mora imati certifikate:

- ISO/IEC 27001:2022 vodeći revizor (upravljanje informacijskom i kibernetičkom sigurnošću),
- ISO 22301:2019 vodeći revizor (upravljanje kontinuitetom poslovanja)
- ISO/IEC 27035 razine lead incident manager – upravljanje incidentima informacijske sigurnosti
- NIS2 vodeći implementator

STRUČNJACI ZA REVIZIJE KIBERNETIČKE SIGURNOSTI I OTPORNOSTI – 2 izvršitelja

U okviru ovog uvjeta tehničke i stručne sposobnosti, svi nominirani stručnjaci iz predmetne grupe moraju

zajedno ispunjavati sve niže navedene uvjete u pogledu kvalifikacija i vještina te općenitog stručnog iskustva.

S obzirom da se radi o kibernetičkoj sigurnosti i otpornosti odnosno kontinuitetu poslovanja te regulatornim specifičnostima, svaki od stručnjaka mora imati certifikate:

- ISO/IEC 27001:2022 vodeći revizor (upravljanje informacijskom i kibernetičkom sigurnošću),
- ISO 22301:2019 vodeći revizor (upravljanje kontinuitetom poslovanja)
- NIS2 vodeći implementator

Jedan stručnjak može posjedovati više certifikata

Općenito stručno iskustvo za gore navedene stručnjake:

Najmanje dvije godine radnog iskustva u okviru provođenja istih ili sličnih vrsta revizije i upravljanja rizicima u području mrežnih i informacijskih sustava odnosno informacijske i kibernetičke sigurnosti i otpornosti, što dokazuju životopisom s popisom projekata.

Kao dokaz da raspolaže navedenim stručnjacima, Izvršitelj će dostaviti Izjavu da raspolaže s osobama odgovarajuće kvalifikacije koje posjeduju strukovnu sposobnost, stručno znanje i iskustvo potrebno za izvršavanje predmeta nabave, te dostaviti Priloge Izjavi kojima to dokazuje. Navedeni stručnjaci moraju biti uključeni u izvršavanje predmeta nabave cijelo vrijeme trajanja ugovora.

Izjavu daje ovlaštena osoba gospodarskog subjekta.

- Izjava sadrži ili joj se prilaže popis stručnjaka u kojem za svakog stručnjaka treba biti navedeno:
- ime i prezime
- navod o stručnoj kvalifikaciji i iskustvu stručnjaka
- navod da će svi navedeni stručnjaci biti raspoloživi gospodarskom subjektu za cijelo vrijeme izvršenja predmeta nabave.

U prvom prilogu Izjave potrebno je za navedene stručnjake dostaviti certifikate o stečenom znanju pri čemu jedan stručnjak može biti nositelj više certifikata.

U drugom prilogu Izjave potrebno je dostaviti Životopis za svakog pojedinog stručnjaka kojim dokazuju svoje općenito stručno iskustvo s navodom najmanje tri ista ili slična projekta na kojima je stručnjak radio, od čega minimalno jedan od ta tri projekta mora biti za sektor zdravstva odnosno laboratorijskih usluga. Potrebno je navesti naziv projekta, ime druge ugovorne strane, kratki opis projekta, navod o trajanju projekta te kontakt za provjeru navoda kod druge ugovorne strane. Zbog navođenja projekata na životopisima stručnjaka, na ovaj Prilog Izvršitelj može staviti oznaku Povjerljivo.

Certifikati se prilažu kao preslike.

Svi certifikati moraju biti izdani od strane akreditiranog certifikacijskog tijela (ako se radi o ISO/IEC standardima) ili relevantnih svjetskih stručnih organizacija ako se radi o ostalim certifikatima.

U slučaju da ponuditelj prilaže jednakovrijedne certifikate dužan je priložiti dokaze iz kojih će Naručitelju biti razvidno da je priloženi certifikat zaista jednakovrijedan, odnosno da je istog (ili višeg) nivoa stručnosti za opseg stručnih kompetencija u odnosu na traženi certifikat te da je izdan od strane organizacije koje su nositelji vlastite međunarodno priznate sheme certificiranja.

Izvršitelj mora na izvršenju ugovora angažirati minimalno stručnjake koje je nominirao u svojoj ponudi, te

za koje je dokazao da imaju tražene uvjete tehničke i stručne sposobnosti. Ukoliko se pokaže potreba za angažmanom ostalih stručnjaka koji posjeduju određena stručna znanja, Izvršitelj ih može angažirati prilikom izvršenja ugovora.

Izvođač može predložiti zamjenu stručnjaka koje je nominirao u ponudi uslijed, primjerice, ali ne isključivo, dugotrajne nesposobnosti za rad stručnjaka, prestanka radnog odnosa stručnjaka i drugih važnih razloga. Predložene zamjene moraju ispunjavati minimalno one uvjete koje ima stručnjak za čiju su zamjenu predloženi.