REPUBLIKA HRVATSKA
DRŽAVNA KOMISIJA ZA KONTROLU POSTUPAKA JAVNE NABAVE

KLASA: UP/II-034-02/26-01/264
URBROJ: 354-02/8-26-8
Zagreb, 11. lipnja 2026.

Državna komisija za kontrolu postupaka javne nabave, Zagreb, OIB: 95857869241, u Vijeću sastavljenom od članova: Danijele Antolković, zamjenice predsjednice te Sanje Badrov Ranić i Marijane Gortan Krnić, članica, postupajući povodom žalbe žalitelja CompING d.o.o., Zagreb, OIB: 09201087238, izjavljenoj u odnosu na odluku o odabiru u otvorenom postupku javne nabave, broj objave: 2026/S F05-0000348, predmet nabave: sustav za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima 2026, naručitelja Plinacro d.o.o., Zagreb, OIB: 69401829750, 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. Poništava se Odluka o odabiru Broj: PN-Z-076/26-MHŠ, od 21. travnja 2026. godine, u otvorenom postupku javne nabave, broj objave: 2026/S F05-0000348, predmet nabave: sustav za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima 2026, naručitelja Plinacro d.o.o., Zagreb.

2. Nalaže se naručitelju, Plinacro d.o.o., Zagreb, da u roku od 8 dana od dana javne objave rješenja na internetskim stranicama Državne komisije za kontrolu postupaka javne nabave naknadi žalitelju CompING d.o.o., Zagreb, troškove žalbenog postupka, u iznosu od 1.534,38 eura.

O b r a z l o ž e n j e

Naručitelj Plinacro d.o.o., Zagreb, objavio je 4. ožujka 2026. godine u Elektroničkom oglasniku javne nabave Republike Hrvatske (dalje u tekstu: EOJN RH) poziv na nadmetanje s dokumentacijom o nabavi u otvorenom postupku javne nabave, broj objave: 2026/S F05-0000348, predmet nabave: sustav za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima 2026. Kriterij odabira je ekonomski najpovoljnija ponuda koja se određuje na temelju kriterija cijene u omjeru 90% te broja stručnjaka s važećim certifikatom proizvođača/ovlaštenog predstavnika/distributera u omjeru 10%.

U predmetnom postupku javne nabave dostavljene su dvije ponude, koje je naručitelj u postupku pregleda i ocjene ponuda ocijenio kao valjane te je Odlukom o odabiru Broj: PN-Z-076/26-MHŠ, od 21. travnja 2026. godine, odabrao ponudu gospodarskog subjekta CS Computer Systems d.o.o., Zagreb, kao ekonomski najpovoljniju.

Na predmetnu odluku o odabiru, koju je naručitelj 22. travnja 2026. godine objavio u EOJN RH, žalbu je 4. svibnja 2026. godine Državnoj komisiji za kontrolu postupaka javne nabave izjavio ponuditelj CompING d.o.o., Zagreb. Žalitelj u žalbi u bitnom osporava valjanost ponude odabranog ponuditelja, žalbenim zahtjevom traži poništenje odluke o odabiru te naknadu troškova žalbenog postupka. Žalitelj je žalbu uredio podneskom zaprimljenim kod ovog državnog tijela 8. svibnja 2026. godine.

Naručitelj u odgovoru na žalbu u bitnom navodi da je ponuda odabranog ponuditelja u cijelosti izrađena u skladu s uvjetima i zahtjevima dokumentacije o nabavi, da su žalbeni navodi neosnovani te predlaže žalbu odbiti.

Odabrani ponuditelj, gospodarski subjekt CS Computer Systems d.o.o., Zagreb, tijekom žalbenog postupka nije se očitovao na navode iz žalbe i naručiteljevog odgovora na žalbu.

U tijeku postupka pred ovim tijelom izvedeni su dokazi pregledom i analizom dokaznog materijala koji se sastoji od dokumentacije o nabavi, zapisnika o otvaranju te pregledu i ocjeni ponuda, odluke o odabiru, ponude odabranog ponuditelja te ostalih dokaza.

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

Žalba je osnovana.

Žalitelj navodi da ponuda odabranog ponuditelja nije sukladna s tehničkim zahtjevima zbog ograničenja broja forenzičkih istraga.

Ističe da su u dokumentu odabranog ponuditelja iz ponude, 13_Funkcijska podloga_ispunjeno.xls, u stupcu Ponuđene karakteristike za redne brojeve 5. do 32. navedeni nazivi ponuđenih proizvoda kako slijedi: Cortex XDR Pro, Cortex XDR Pro for daily ingested GB, Annual Forensics add-on.

Nadalje, u dokumentu odabranog ponuditelja iz ponude, 14_Tehnička specifikacija ponuđenog rješenja.pdf, sadržan je opis navedenih proizvoda, pri čemu odabrani ponuditelj navodi da isti udovoljavaju traženim tehničkim specifikacijama.

Međutim, žalitelj ukazuje da je Annual Forensics add-on, koji odabrani ponuditelj nudi kao dio rješenja, ograničen na najviše 50 forenzičkih istraga. Ističe da je naručitelj zahtijevao udaljeno prikupljanje forenzičkih artefakata nad svim uređajima bez ograničenja (520 uređaja) pa uvedeno kvantitativno ograničenje, po mišljenju žalitelja onemogućuje potpuno provođenje forenzičkih radnji u slučaju incidenta koji zahvaća širi dio infrastrukture. Žalitelj smatra da je time narušeno načelo jednakog tretmana, jer je žalitelj, koji je ispunio taj zahtjev bez ograničenja, doveden u nepovoljniji položaj.

Naručitelj u odgovoru na žalbu uvodno ističe da je predmet otvorenog postupka javne nabave nabava cjelovitog Sustava za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima 2026 sukladno načelu „isporuka do pune funkcionalnosti bez dodatnih troškova za naručitelja“, a što je jasno istaknuto u više dijelova dokumentacije o nabavi (Obavijest o nadmetanju, točke 3. i 4., Dio I - Opći podaci o postupku nabave, točka 3., Tehnička podloga (više različitih točaka), Prijedlog ugovora, stavak 1.2.).

Ističe da je predmet nabave, uključujući i funkcionalnosti, detaljno opisao u dokumentu Tehnička podloga. Tako je pod točkom 3.3. dokumenta Tehnička podloga, naručitelj propisao da nabavlja licence za 320 krajnjih uređaja i 200 poslužitelja, dakle

ukupno 520 licenci, pri čemu je izričito razlikovao 500 licenci sa standardnom zaštitom i minimalno 20 licenci s uključenom naprednom zaštitom. Za licence s uključenom naprednom zaštitom, naručitelj je pod istom točkom dokumenta Tehnička podloga naveo da će samostalno definirati na koje krajnje uređaje i poslužitelje će licence s uključenom naprednom zaštitom biti instalirane.

Dakle, iz navedenog je razvidno, smatra naručitelj, da je zahtijevao minimalno 20 licenci s uključenom naprednom zaštitom, a ne neograničenu primjenu svih naprednih funkcija na svih 520 krajnjih uređaja i poslužitelja. Ukazuje da su moduli/funkcije licenci s uključenom naprednom zaštitom, a koji su u bitnom predmet ovog žalbenog postupka, propisani u istom dijelu dokumenta Tehnička podloga, točkama a) do h). Za dokazivanje dijela traženih funkcionalnosti, primarno u odnosu na module/funkcije licenci s uključenom standardnom zaštitom, naručitelj je izradio dokument Funkcijska podloga kojeg su ponuditelji bili obvezni popuniti te zajedno s dokumentom kojim se dokazuje tražena funkcionalnost dostaviti u sklopu ponude.

Iz navedenog proizlazi, ukazuje naručitelj, da dokumentom Funkcijska podloga nije predviđeno dokazivanje svih zahtjeva u odnosu na module/funkcije licenci s uključenom naprednom zaštitom propisane pod točkama a) do h). Stoga su ponuditelji u svojoj ponudi morali dokazati isključivo zahtjeve propisane Funkcijskom podlogom.

Također, naručitelj ističe da u dokumentaciji o nabavi nije propisao obvezu navođenja i dokazivanja konkretne tehnologije provedbe pojedine funkcionalnosti, niti navođenje konkretne proizvođačke licence, podlicence, module ili add-onova kojima se pojedina funkcionalnost mora ostvariti. Svi zahtjevi su bili postavljeni funkcionalno, odnosno kao tražene mogućnosti koje ponuđeno rješenje mora omogućiti, dok je izbor tehničkog načina provedbe, licenčnog modela i potrebnih komponenti bio na ponuditelju, uz obvezu da ponuđeno rješenje bude isporučeno do pune funkcionalnosti i bez dodatnih troškova za naručitelja.

Sukladno prethodno opisanim zahtjevima, naručitelj ističe da je ponude pregledao u skladu s odredbama dokumentacije o nabavi te je prilikom pregleda i ocjene ponude ocjenjivao isključivo funkcionalnosti tražene u dokumentu Funkcijska podloga.

Što se tiče konkretnog žalbenog navoda, naručitelj ističe da je dokazivanje funkcionalnosti forenzičnih istraga propisano dokumentom Funkcijska podloga, a navedena funkcionalnost se dokazuje u okviru 20 licenci s uključenom naprednom zaštitom. Kao odlučno ističe da broj paralelnih forenzičkih istraga nad svih 520 krajnjih uređaja i poslužitelja dokumentacijom o nabavi nije propisan.

Ukazuje da je vezano za forenzične istrage, odabrani ponuditelj u dostavljenoj ponudi, dokument „13_Funkcijska podloga_ispunjeno.xlsx“, za funkcionalnost Forenzika - Sustav mora omogućiti udaljeno prikupljanje forenzičkih artefakata (uključujući podatke o aktivnim procesima, mrežnim vezama, registru i sistemskim zapisima) te podržavati prikupljanje sadržaja radne memorije“ označio odgovor „DA“ te je kao ponuđene proizvode naveo Cortex XDR Pro, Cortex XDR Pro for daily ingested GB i Annual Forensics addon.

Naručitelj ističe da je funkcionalnost prikupljanja forenzičkih podataka potvrđena u dokumentu „CortexXDR_dokumentacija.pdf“, stranici 750., gdje je navedena funkcionalnost „Monitor and Collect Forensics Data“, uz napomenu da je za korištenje potrebna Forensics Add-on licenca. U tom dijelu dokumentacije navedeno je da Cortex XDR agent prikuplja detaljne informacije o tome što se dogodilo na krajnjem uređaju ili poslužitelju radi stvaranja forenzičke baze, uključujući podatke iz kategorija kao što su Process Execution, File Access, Persistence, Command History, Network, Remote Access i Search Collections. Naručitelj zaključuje da je time potvrđeno da ponuđeno rješenje omogućuje udaljeno prikupljanje forenzičkih artefakata, uključujući podatke o procesima i mrežnim aktivnostima.

Dodatno, ukazuje da je u dokumentu „CortexXDR_dokumentacija.pdf', stranici 1174. u poglavlju koje se odnosi na prikupljanje slike memorije, odnosno „Collect a memory image“, navedeno da funkcionalnost zahtijeva Cortex XDR Pro i Forensics add-on licencu te omogućuje prikupljanje memorijske slike krajnjeg uređaja ili poslužitelja radi daljnje forenzičke analize. Time je po mišljenju naručitelja potvrđeno da ponuđeno rješenje podržava i prikupljanje sadržaja radne memorije.

Nadalje, ističe da je u dokumentu „CortexXDR_dokumentacija.pdf“, stranica 1175. dodatno opisano da se forenzičke istrage sastoje od jedne ili više kolekcija podataka s krajnjih uređaja i poslužitelja te da se kroz Hunt collections i Triage collections mogu prikupljati i analizirati relevantni forenzički artefakti. Posebno je važno da dokumentacija navodi kako Triage collections omogućuju prikupljanje trenutno podržanih forenzičkih artefakata, uključujući korisnički definirane putanje datoteka, pune popise datoteka, event logove i registry hives, čime su pokriveni i sistemski zapisi i registar, kako je bilo traženo.

U dokumentu „Tehnička specifikacija ponuđenog rješenja — Palo Alto Cortex xdr“, stranica 1., ponuditelj je naveo da nudi Cortex XDR Pro for 1 endpoint za ukupno 520 krajnjih uređaja i poslužitelja u trajanju od 36 mjeseci, kao i Annual Forensics add-on for 1 Cortex XDR endpoint, odnosno pretplatu za forenzičke potrebe koja omogućuje provođenje do 50 istovremenih forenzičkih istraga. Naručitelj pojašnjava da iz navedene formulacije proizlazi da se ograničenje odnosi na broj istovremenih forenzičkih istraga, a ne na ukupan broj krajnjih uređaja i poslužitelja koji su pokriveni licencama niti na ukupan broj forenzičkih radnji tijekom trajanja ugovora.

Slijedom navedenog, naručitelj je prihvatio zahtjev kao ispunjen, jer je iz dostavljene ponude razvidno da je odabrani ponuditelj u funkcijskoj podlozi potvrdio ispunjenje zahtjeva, naveo odgovarajuće ponuđene proizvode i dostavio dokumentaciju kojom se potvrđuje da ponuđeno rješenje omogućuje udaljeno prikupljanje forenzičkih artefakata, uključujući procese, mrežne veze, registar, sistemske zapise i sadržaj radne memorije.

Također, iz dostavljene dokumentacije razvidno je da se ponuđeno rješenje licencira za traženi opseg krajnjih uređaja i poslužitelja, dok se ograničenje od 50 istovremenih forenzičkih istraga odnosi isključivo na broj istovremenih forenzičkih istraga. Navedeno ograničenje ne predstavlja odstupanje od zahtjeva dokumentacije o nabavi, osobito zato što je dokumentom Tehnička podloga propisano minimalno 20 licenci s naprednom zaštitom, a ne neograničen broj paralelnih forenzičkih istraga nad svih 520 krajnjih uređaja i poslužitelja. Budući je odabrani ponuditelj dokazao da ispunjava uvjet propisan Funkcijskom podlogom, činjenica da je žalitelj ponudio funkcionalnost bez ograničenja, ne predstavlja povredu načela jednakog tretmana, zaključuje naručitelj u odgovoru na žalbu.

U očitovanju na naručiteljev odgovor na žalbu žalitelj ističe da postojanje ograničenja broja paralelnih odnosno istovremenih forenzičkih aktivnosti, dokumentacijom o nabavi nigdje nije propisano kao dopušteno funkcionalno ograničenje broja simultanih forenzičkih istraga niti je predviđen prihvatljiv prag takvog ograničenja. Štoviše, tehnički zahtjev formuliran je općenito i bez kvalifikacija, odnosno naručitelj je zahtijevao sustav koji „mora omogućiti udaljeno prikupljanje forenzičkih artefakata (...) te podržavati prikupljanje sadržaja radne memorije”, bez ikakvog navođenja da se navedene funkcionalnosti mogu izvršavati uz numeričko ograničenje broja istovremenih aktivnosti. Iz tako formuliranog zahtjeva, po mišljenju žalitelja proizlazi da je naručitelj tražio funkcionalno rješenje koje omogućuje neometano provođenje navedenih aktivnosti, pri čemu dokumentacija o nabavi ne predviđa niti izričito niti implicitno prihvatljivo ograničenje broja paralelnih forenzičkih istraga.

Potom žalitelj ističe da naručitelj u svom odgovoru tumači ovo ograničenje kao ograničenje broja istovremenih istraga (ne broja endpointa), zaključujući da to nije odstupanje od zahtjeva dokumentacije o nabavi, jer njome nije propisivao broj paralelnih

istraga. Međutim, osim ograničenja od 50 istovremenih istraga na koje se poziva naručitelj, žalitelj ukazuje da dokumentacija proizvođača sadrži i dodatno, funkcionalno značajno ograničenje vezano uz sam triage postupak, a koji je naručitelj u odgovoru potpuno zaobišao. U samoj Cortex XDR dokumentaciji odabranog ponuditelja (CortexXDR_dokumentacija.pdf, stranica 1175) opisano je tehničko ograničenje prema kojem količina podataka prikupljenih tijekom trijaže (triage) može biti velika, zato su triage kolekcije ograničene na deset ili manje krajnjih točaka (endpoint) po kolekciji. Žalitelj pojašnjava da navedeno ograničenje od 10 endpointa po triage kolekciji nije administrativno ograničenje konfiguracijske prirode već arhitekturalno ograničenje samog sustava, eksplicitno navedeno u dokumentaciji proizvođača. Triage kolekcija je temeljni alat za dubinsko forenzičko prikupljanje artefakata s endpointa (aktivni procesi, registry, mrežne veze, event logovi), što odgovara upravo zahtjevu iz Funkcijske podloge.

Smatra da budući da predmet nabave obuhvaća ukupno 520 krajnjih uređaja i poslužitelja, kombinacija ograničenja od 50 istovremenih istraga i 10 endpointa po triage kolekciji stvara funkcionalno ograničenje relevantno za infrastrukturu naručitelja. U scenariju incidenta većeg opsega sustav zahtijeva serijalizaciju forenzičkih radnji (provođenje triagea u serijskim grupama od 10 uređaja), što nije funkcionalno ekvivalentno istovremenom prikupljanju artefakata sa svih zahvaćenih uređaja. Svako kašnjenje u prikupljanju forenzičkih dokaza povećava rizik od gubitka volatilnih podataka (sadržaj radne memorije, aktivni mrežni procesi) koji su ključni za utvrđivanje uzroka i opsega napada.

Žalitelj ilustrira opisani problem pomoći tablice te ističe da tablica pokazuje da je ponuđeno rješenje funkcionalno adekvatno samo za incidente malog opsega. Međutim, da u scenariju masivnog ransomware napada, koji je upravo scenarij koji naručiteljeva Tehnička podloga ima na umu pri postavljanju zahtjeva za forenzičkim kapacitetom, sustav ne može istovremeno provesti triage nad svim zahvaćenim uređajima.

Ocjenjujući žalbeni navod izvršen je uvid u odgovarajuće dijelove dokumentacije o nabavi, na koje uostalom upućuju i stranke žalbenog postupka.

Sastavni dio dokumentacije o nabavi je dokument naslova Tehnička podloga, u kojemu je u točki 3.3. Licence i tehnička podrška, propisano sljedeće:

„Usluga obuhvaća nabavu licenci i tehničku podršku s uključenim održavanjem za sustav za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima. Cilj je osigurati pravovremenu aktivaciju licenci, dostupnost podrške proizvođača te neprekidnu funkcionalnost sustava tijekom trajanja licenci. Licence se aktiviraju prilikom instalacije, konfiguracije i puštanja sustava u rad, te vrijede 36 mjeseci od datuma aktivacije. Licence se nabavljaju za 320 krajnjih uređaja (računala) i 200 poslužitelja (ukupno 520 licenci), s funkcionalnostima kako slijedi:

1. 500 licenci s uključenom standardnom zaštitom opisanom u dokumentu „Funkcijska podloga“,

2. Minimalno 20 licenci s uključenom naprednom zaštitom koja uključuje module/funkcije:

a. Ove licence moraju imati mogućnost instalacije i korištenja na krajnjim uređajima (računalima) i poslužiteljima (Windows i Linux).

b. Agent-based ili agentless antimalware zaštita uz analizu datoteka u oblaku i praćenje sumnjivih obrazaca ponašanja u stvarnom vremenu,

c. Proaktivnu zaštitu poslužiteljskih aplikacija i operacijskih sustava od poznatih i "zero-day" ranjivosti putem sustava za sprječavanje upada na razini hosta (Host IPS),

d. Napredni mehanizmi detekcije ransomwarea uz automatsko kreiranje backup kopija datoteka povrata,

e. Naprednu mrežnu kontrolu s dvosmjernim vatrozidom s praćenjem stanja (stateful firewall), te naprednom zaštitom od tuneliranja i premošćivanja mrežnih okruženja,

f. Filtriranje i blokiranje pristupa malicioznim internet domenama izravno na razini hipervizora,
g. Kontinuirani nadzor integriteta datoteka (File Integrity Monitoring - FIM) te dubinska analiza sistemskih zapisa (logova)
h. Naručitelj će samostalno definirati na koje krajnje uređaje i poslužitelje će licence biti instalirane.
3. Nabava licenci potrebnih za rad 10 agenata;

Sastavni dio dokumentacije o nabavi je također i dokument Funkcijska podloga, u kojem su opisane tražene funkcionalnosti sustava, predviđeno mjesto za upis potvrde traženih funkcionalnosti/karakteristika ponuđenog predmeta nabave te upis podatka o broju stranice dokumenta koji se dostavlja kao dokaz potvrde tražene funkcionalnosti/karakteristike.

Uzevši u obzir žaliteljev žalbeni navod, ovdje treba citirati traženu funkcionalnost Forenzika, opisanu pod rednim brojem 29. Funkcijske podloge, na sljedeći način: Sustav mora omogućiti udaljeno prikupljanje forenzičkih artefakata (uključujući podatke o aktivnim procesima, mrežnim vezama, registru i sistemskim zapisima) te podržavati prikupljanje sadržaja radne memorije.

Odabrani ponuditelj je u ponudi dostavio dokument naslova Specifikacija ponuđenog rješenja – Palo Alto Cortex XDR, u kojemu je navedeno sljedeće:

„1. Cortex XDR Pro for 1 endpoint, includes 30 days of data retention and standard success; 3 year. Pretplata (licenca) i standardna success podrška proizvođača za ukupno 520 krajnjih uređaja i poslužitelja u trajanju od 36 mjeseci od datuma aktivacije pretplate. Standardna success podrška proizvođača uključuje sljedeće: rješavanje tehničkih problema i incidenata, siguranje prava na sve nove verzije sustava, nadogradnje funkcionalnosti, sigurnosne zakrpe i redovita ažuriranja.

2. Annual Forensics add-on for 1 Cortex XDR endpoint, includes 30 days of data retention; 3 year. Pretplata (licenca) za forenzičke potrebe, koja omogućuje provođenje do 50 istovremenih forenzičkih istraga, uz standardnu success podršku proizvođača u trajanju od 36 mjeseci od datuma aktivacije pretplate. Standardna success podrška proizvođača obuhvaća rješavanje tehničkih problema i incidenata, pravo na sve nove verzije sustava, nadogradnje funkcionalnosti, kao i redovite sigurnosne zakrpe i ažuriranja.

3. Cortex XDR Pro for daily ingested GB. Includes 30 days of ingested data retention, 180 days of alerts and incidents retention and standard success; 3 year. Pretplata (licenca) koja uključuje dnevni unos podataka u platformu u iznosu od 33 GB, uz standardnu success podršku proizvođača u trajanju od 36 mjeseci od datuma aktivacije pretplate. Standardna success podrška proizvođača obuhvaća rješavanje tehničkih problema i incidenata, pravo na sve nove verzije sustava, nadogradnje funkcionalnosti, kao i redovite sigurnosne zakrpe i ažuriranja.“.

Za ocjenu žalbenog navoda mjerodavne su odredbe članka 280. stavka 4., članka 290. stavka 1. i članka 403. ZJN 2016.

Žalitelj žalbeni navod temelji na podatku iz dokumenta Specifikacija ponuđenog rješenja – Palo Alto Cortex XDR, u kojemu je odabrani ponuditelj naveo tri sastavna dijela ponuđenog sustava, gdje u odnosu na licencu Annual Forensics add-on stoji da ona omogućuje provođenje do 50 istovremenih forenzičkih istraga. U odnosu na žalbeni navod da navedeno ograničenje čini ponudu neusklađenom s dokumentacijom o nabavi, Državna komisija prihvaća argumentaciju naručitelja da dokumentacijom o nabavi nije propisan broj paralelnih ili istovremenih forenzičkih istraga, niti je propisana obveza neograničenog provođenja takvih radnji na svim krajnjim uređajima i poslužiteljima. Naime, naručitelj je zahtjeve postavio funkcionalno, odnosno kroz opis mogućnosti koje sustav mora omogućiti, bez propisivanja načina njihove implementacije, licencnog modela ili kvantitativnih

parametara poput broja istovremenih forenzičkih istraga. Također, iz dokumentacije o nabavi proizlazi da se predmetna funkcionalnost odnosi na licence s uključenom naprednom zaštitom, kojih je naručitelj zahtijevao minimalno 20, a ne na svih 520 krajnjih uređaja i poslužitelja. Slijedom toga, nije osnovan zaključak žalitelja da bi sustav morao omogućiti istovremeno provođenje forenzičkih radnji nad svim uređajima bez ikakvih ograničenja.

Nadalje, činjenica da ponuđeno rješenje predviđa ograničenje od 50 istovremenih forenzičkih istraga ne može se smatrati odstupanjem od zahtjeva dokumentacije o nabavi, budući da takvo ograničenje dokumentacijom nije zabranjeno niti je definiran minimalni prag istovremenosti. Stoga navedeno ograničenje predstavlja dio tehničkog i licencnog modela ponuđenog rješenja, koji je u skladu s postavljenim funkcionalnim zahtjevima naručitelja.

U odnosu na navod žalitelja o povredi načela jednakog tretmana, Državna komisija utvrđuje da okolnost da je žalitelj eventualno ponudio rješenje bez navedenog ograničenja ne znači da je naručitelj bio obvezan odbiti ponudu odabranog ponuditelja, budući da dokumentacijom o nabavi nije propisao takav zahtjev. Naime, naručitelj je dužan ocjenjivati ponude isključivo prema unaprijed propisanim uvjetima i zahtjevima, a ne prema dodatnim kriterijima koji nisu bili sastavni dio dokumentacije o nabavi. Slijedom navedenog, Državna komisija ocjenjuje da žalitelj nije dokazao da ponuđeno rješenje odabranog ponuditelja ne udovoljava traženim funkcionalnim zahtjevima, niti da je naručitelj postupio protivno odredbama dokumentacije o nabavi kada je predmetni zahtjev ocijenio ispunjenim.

U odnosu na dodatne navode žalitelja iz naknadno dostavljenog očitovanja, koji se odnose na ograničenja vezana uz tzv. triage kolekcije i broj krajnjih točaka po kolekciji, Državna komisija utvrđuje da se radi o novim žalbenim navodima koji nisu bili istaknuti u žalbi, već su izneseni tek u naknadnom očitovanju žalitelja na odgovor naručitelja na žalbu. Budući da sukladno relevantnim odredbama ZJN 2016 žalitelj nakon isteka roka za izjavljivanje žalbe ne može iznositi nove žalbene navodi, navedeni navodi su zakašnjeli te ih žalbeni tijelo stoga nije uzelo u razmatranje.

Slijedom svega navedenog, predmetni žalbeni navod ocijenjen je neosnovanim.

Žalitelj dalje u žalbi navodi da ponuda odabranog ponuditelja nije sukladna s tehničkim zahtjevima zbog ograničenja dnevnog volumena podataka. Ističe da su u dokumentu odabranog ponuditelja iz ponude, 13_Funkcijska podloga_ispunjeno.xls, u stupcu ponuđene karakteristike za redne brojeve 5 do 32, navedeni nazivi ponuđenih proizvoda kako slijedi: Cortex XDR Pro, Cortex XDR Pro for daily ingested GB, Annual Forensics add-on.

Nadalje, u dokumentu odabranog ponuditelja iz ponude, 14_Tehnička specifikacija ponuđenog rješenja.pdf, sadržan je opis navedenih proizvoda, pri čemu odabrani ponuditelj navodi da isti udovoljavaju traženim tehničkim specifikacijama. Žalitelj ističe da ponuđeno rješenje Cortex XDR Pro for daily ingested GB, ograničava dnevni unos podataka u platformu na 33 GB. Kako funkcionalnost sustava izravno ovisi o tom promjenjivom faktoru (volumenu prometa), žalitelj zaključuje da je odabrani ponuditelj de facto ponudio uvjetovano rješenje, iako je naručitelj u tehničkoj specifikaciji zahtijevao ispunjenje svih traženih funkcionalnosti bez ograničenja, za sve uređaje naručitelja. Stoga smatra da je ovim propustom naručitelj povrijedio načela jednakog tretmana i transparentnosti.

Naručitelj u odgovoru na žalbu navodi da u dokumentu Tehnička podloga nije propisao zahtjev za neograničenim dnevnim unosom podataka u platformu i minimalni dnevni volumen podataka koji ponuđeno rješenje mora podržavati. Vezano za dnevni volumen podataka, ističe da je odabrani ponuditelj u ponudi, dokumentu Tehnička specifikacija ponuđenog rješenja - Palo Alto Cortex xdr, naveo da nudi Cortex XDR Pro for

daily ingested GB, odnosno pretplatu koja uključuje „dnevni unos podataka u platformu u iznosu od 33 GB“. Naručitelj smatra da je time odabrani ponuditelj jasno i transparentno iskazao licenčni kapacitet dnevnog unosa podataka u platformu. Budući naručitelj dokumentacijom o nabavi nije propisao neograničeni dnevni unos podataka u platformu i minimalni dnevni volumen podataka koji ponuđeno rješenje mora podržavati, navedeni kapacitet od 33 GB dnevnog unosa podataka ne predstavlja odstupanje od zahtjeva dokumentacije o nabavi. Slijedom navedenog, činjenica da je žalitelj ponudio funkcionalnost bez ograničenja, ne predstavlja povredu načela jednakog tretmana, zaključuje naručitelj u odgovoru na žalbu.

U očitovanju na naručiteljev odgovor na žalbu, žalitelj ističe da je predmet nabave definiran kao „Sustav za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima”, iz čega bi proizlazilo da je svrha sustava osigurati cjelovitu, kontinuiranu i fleksibilnu detekciju i forenzičku analizu sigurnosnih događaja na razini većeg broja krajnjih uređaja i poslužiteljskih sustava, uključujući mogućnost obrade značajnih količina sigurnosno relevantnih podataka. Slijedom navedenoga, iako dokumentacija o nabavi ne propisuje izričito minimalni dnevni volumen podataka, takva okolnost, po mišljenju žalitelja, ne može se tumačiti na način da je dopušteno uvođenje ograničenja koja objektivno ograničavaju sposobnost sustava da ispuni svrhu nabave. Pojašnjava da ograničenje dnevnog unosa podataka od 33 GB predstavlja kvantitativno ograničenje obrade podataka koje, u kontekstu sveobuhvatnog otkrivanja prijetnji u okruženju velikih informacijskih sustava, može dovesti do nepotpunog prikupljanja i analize sigurnosnih artefakata, osobito u scenarijima distribuiranih ili višestrukih sigurnosnih incidenata. Stoga žalitelj smatra da se tehnički zahtjevi dokumentacije o nabavi moraju tumačiti u skladu sa svrhom predmeta nabave, odnosno na način da sustav mora biti sposoban obraditi sve relevantne sigurnosne podatke koji proizlaze iz operativnog okruženja naručitelja, bez unaprijed definiranih ograničenja koja bi mogla kompromitirati sveobuhvatnost detekcije prijetnji.

U rješenju je već utvrđeno da je odabrani ponuditelj sastavne dijelove ponuđenog sustava opisao u dokumentu Specifikacija ponuđenog rješenja – Palo Alto Cortex XDR, iz sadržaja kojega treba ponoviti da je pod točkom 3. opisan Cortex XDR Pro for daily ingested GB. Includes 30 days of ingested data retention, 180 days of alerts and incidents retention and standard success; 3 year, odnosno pretplata (licenca) koja uključuje dnevni unos podataka u platformu u iznosu od 33 GB, uz standardnu success podršku proizvođača u trajanju od 36 mjeseci od datuma aktivacije pretplate.

Za ocjenu žalbenog navoda mjerodavne su odredbe članka 280. stavka 4., članka 290. stavka 1. i članka 403. ZJN 2016.

Kako je utvrđeno prethodno u rješenju, iz sadržaja dokumentacije o nabavi proizlazi da je naručitelj u dokumentu Tehnička podloga propisao predmet nabave kao sustav za sveobuhvatno otkrivanje prijetnji na krajnjim uređajima i poslužiteljima, uz definiranje potrebnih licenci i funkcionalnosti sustava. Međutim, pregledom predmetne dokumentacije o nabavi nije utvrđeno da je naručitelj propisao zahtjev koji se odnosi na neograničen dnevni unos podataka u platformu, niti je odredio minimalni dnevni volumen podataka koji ponuđeno rješenje mora podržavati. Uvidom u ponudu odabranog ponuditelja utvrđeno je da je isti u dokumentu Specifikacija ponuđenog rješenja – Palo Alto Cortex XDR naveo da nudi komponentu Cortex XDR Pro for daily ingested GB, pri čemu je izričito naznačeno da ponuđena pretplata uključuje dnevni unos podataka u platformu u iznosu od 33 GB. Time je odabrani ponuditelj jasno i transparentno iskazao kapacitet ponuđenog rješenja u pogledu dnevnog unosa podataka.

U odnosu na žalbeni navod, Državna komisija prihvaća argumentaciju naručitelja da, s obzirom na to da dokumentacijom o nabavi nije propisan zahtjev u pogledu neograničenog dnevnog unosa podataka niti minimalni prag dnevnog volumena podataka,

navedeni podatak iz ponude odabranog ponuditelja ne može predstavljati odstupanje od zahtjeva dokumentacije o nabavi. Naime, naručitelj je tehničke zahtjeve definirao funkcionalno, bez propisivanja konkretnih kvantitativnih parametara koji se odnose na količinu podataka koju sustav mora obrađivati na dnevnoj razini. Slijedom navedenog, okolnost da ponuđeno rješenje uključuje određeni licencni kapacitet dnevnog unosa podataka ne znači da ono ne ispunjava tražene funkcionalnosti, budući da dokumentacija o nabavi nije sadržavala zahtjev kojim bi se takvo ograničenje zabranilo ili propisao minimalni potrebni kapacitet.

U odnosu na daljnje navode žalitelja kojima ukazuje na svrhu predmeta nabave i potrebu obrade velikih količina podataka, Državna komisija ističe da se ponude u postupku javne nabave ocjenjuju isključivo u odnosu na zahtjeve kako su oni propisani dokumentacijom o nabavi, a ne prema naknadnim tumačenjima svrhe ili očekivanjima koja nisu izričito normirana. Stoga se općenito pozivanje žalitelja na svrhu sustava i potrebu „sveobuhvatnosti“ ne može smatrati dostatnim za utvrđenje nesukladnosti ponude odabranog ponuditelja, u situaciji kada konkretni tehnički zahtjev u tom dijelu nije bio preciziran. Također, okolnost da je žalitelj eventualno ponudio rješenje bez ograničenja dnevnog unosa podataka ne dovodi do zaključka o povredi načela jednakog tretmana, budući da naručitelj nije takvu karakteristiku propisao dokumentacijom o nabavi.

Slijedom svega navedenog, Državna komisija ocjenjuje da žalitelj nije dokazao da ponuđeno rješenje odabranog ponuditelja odstupa od zahtjeva dokumentacije o nabavi, te se predmetni žalbeni navod ocjenjuje neosnovanim.

Žalitelj dalje u žalbi navodi da je ponuda odabranog ponuditelja nesukladna s tehničkim zahtjevima jer nije dokazana funkcionalnost naprednih licenci. Ukazuje da Tehnička podloga u točki 3.3. (Licence i tehnička podrška) propisuje minimalne tehničke zahtjeve za 20 licenci s naprednom zaštitom, a prema kojoj bi ponuđeno rješenje moralo kumulativno uključivati funkcionalne zahtjeve navedene pod a do g.

Ističe da odabrani ponuditelj nije ni u jednom dijelu ponude dostavio dokaze da ponuđeno rješenje ispunjava svaki od tih zahtjeva pa je naručitelj prihvatljivost ponude ocijenio na temelju puke pretpostavke, što je protivno načelu transparentnosti i obvezi objektivnog pregleda i ocjene ponuda. Na taj način su ostali ponuditelji koji su dostavili dokaze za zahtijevane funkcionalnosti i ponudili rješenje koje ih zadovoljava, stavljeni u nepovoljniji položaj.

Konkretno, žalitelj ističe da funkcionalni zahtjev pod točkom d) Napredni mehanizmi detekcije ransomwarea uz automatsko kreiranje backup kopija datoteka povrata, nije sastavni dio ponuđenog rješenja prema javno dostupnoj dokumentaciji proizvođača ponuđenog rješenja, društva Palo Alto. Pojašnjava da se tražena funkcionalnost automatskog kreiranja backup kopija datoteka povrata pri detekciji ransomwarea može potencijalno ostvariti jedino uz dodatna rješenja koja nisu navedena u odabranoj ponudi, a naručitelj je to propustio utvrditi i provjeriti.

Također, žalitelj ističe da funkcionalni zahtjev pod točkom f) Filtriranje i blokiranje pristupa malicioznim internet domenama izravno na razini hipervizora“ nije moguće ostvariti rješenjem opisanim u ponudi odabranog ponuditelja prema javno dostupnoj dokumentaciji proizvođača. Ističe da se tražena funkcionalnost filtriranja i blokiranja pristupa malicioznim domenama izravno na razini hipervizora može potencijalno ostvariti jedino uz dodatno rješenje koje nije navedeno u odabranoj ponudi. Ukazuje da za tu funkcionalnost proizvođač upućuje na drugi proizvod (Palo Alto VM-Series) koji nije dio ponude odabranog ponuditelja, a što je naručitelj propustio utvrditi.

Naručitelj u odgovoru na žalbu ističe da je već pojasnio da u okviru postupka nabavlja 520 licenci, pri čemu je izričito razlikovao 500 licenci sa standardnom zaštitom i

minimalno 20 licenci s uključenom naprednom zaštitom. Moduli/funkcije licenci s uključenom naprednom zaštitom, detaljno su opisani dokumentacijom o nabavi, dio Tehnička podloga, točka 3.3., moduli/funkcije označene slovima a) do h). Također, naručitelj je već naveo da dokumentom Funkcijska podloga nije predvidio zasebno dokazivanje svih zahtjeva u odnosu na module/funkcije licenci s uključenom naprednom zaštitom propisane pod točkama a) do h).

U nastavku odgovora na žalbu naručitelj daje prikaz zahtjeva naručitelja i dostavljenih dokaza odabranog ponuditelja, u odnosu na sve zahtjeve točke 3.3. od a do h. Ovdje treba reći da uzevši u obzir navode žalitelja iz kojih proizlazi konkretno osporavanje samo točaka d i f , navode naručitelja iz odgovora na žalbu te žaliteljevo naknadno očitovanje, proizlazi da je sporno i da treba ocijeniti udovoljava li ponuđeni sustav odabranog ponuditelja zahtjevima opisanima pod d i f. Naručitelj je u odgovoru na žalbu iscrpno naveo na temelju kojih podataka iz ponude odabranog ponuditelja je ocijenio da je udovoljeno zahtjevima točke 3.3. pod a, b, c, e, g i h, međutim, zbog nepotrebnog opterećenja teksta nije svrhovito iste iznositi u rješenju.

Naručitelj dalje ističe da su u dijelu točke 3.3. pod d. traženi napredni mehanizmi detekcije ransomwarea uz automatsko kreiranje backup kopija datoteka povrata. Prije prikaza dostavljenih dokaza, naručitelj napominje da dokumentacijom o nabavi nije bilo propisano da ponuđeno rješenje mora sadržavati zaseban backup sustav, već je bilo propisano isključivo kreiranje backup kopija datoteka povrata. Nadalje, ukazuje da dokazivanje predmetne funkcionalnosti nije bilo propisano dokumentom Funkcijska podloga. Iako za navedenu funkcionalnost nije bila propisana obveza dokazivanja, naručitelj je prilikom postupka preglede i ocjene ponuda, radi cjelovitog utvrđenja ispunjenja svih traženih zahtjeva, uzeo u obzir dostavljenu tehničku dokumentaciju i utvrdio da je odabrani ponuditelj u svojoj ponudi dostavio sljedeće:

- Dokument „CortexXDR_dokumentacija.pdf", u kojem je na stranici 670.-671., u pregledu zaštitnih funkcionalnosti navedena funkcionalnost „Ransomware protection“, za koju je opisano da omogućuje zaštitu od aktivnosti šifriranja povezanih s ransomware napadima. Time je po mišljenju naručitelja potvrđeno da ponuđeno rješenje uključuje mehanizam zaštite usmjeren upravo na ransomware aktivnosti, odnosno na prepoznavanje i sprječavanje aktivnosti šifriranja koje su karakteristične za ransomware napade.

- Dokument „CortexXDR_dokumentacija.pdf', u kojem je na stranici 676. navedeno da funkcionalnost „Ransomware protection“ cilja aktivnosti šifriranja povezane s ransomwareom radi analize i zaustavljanja ransomwarea prije nastanka gubitka podataka. Time je po mišljenju naručitelja potvrđen dio zahtjeva koji se odnosi na napredne mehanizme detekcije i sprječavanja ransomwarea, jer dokumentacija opisuje analizu ransomware ponašanja i zaustavljanje napada prije gubitka podataka.

- Dokument „CortexXDR_dokumentacija.pdf", u kojem je na stranici 719., u dijelu koji opisuje konfiguraciju „Ransomware Protection“, navedeno da se ta funkcionalnost koristi za zaštitu od aktivnosti šifriranja povezanih s ransomware napadima. Također, navedeno je kada Cortex XDR agent detektira ransomware aktivnost lokalno na krajnjem uređaju ili u unaprijed definiranim mrežnim mapama, agent izvršava konfiguriranu radnju, primjerice Block ili Report. Osim toga, navedena je mogućnost „Quarantine Malicious Process“ i mogućnost „Quarantine Malicious Files“, kojima se procesi povezani s ransomware aktivnošću mogu staviti u karantenu, te se opisuje korištenje decoy files radi detekcije ransomware ponašanja. Time je po mišljenju naručitelja potvrđeno da ponuđeno rješenje omogućuje detekciju, blokiranje i reakciju na ransomware aktivnosti na krajnjim uređajima i poslužiteljima.

- Dokument „CortexXDR_api.pdf', u kojem je na stranici 325. opisana funkcionalnost „Restore File", odnosno mogućnost vraćanja datoteke koja je stavljena u karantenu na

traženom krajnjem uređaju. Time je po mišljenju naručitelja potvrđeno da ponuđeno rješenje podržava funkcionalnost povrata datoteka iz karantene, što je naručitelj uzeo u obzir u kontekstu dijela zahtjeva koji se odnosi na povrat datoteka nakon sigurnosnog događaja.

Slijedom navedenog, naručitelj zaključuje da iz dostavljene dokumentacije proizlazi da ponuđeno rješenje uključuje napredne mehanizme ransomware zaštite, detekciju i zaustavljanje aktivnosti šifriranja, korištenje decoy datoteka, stavljanje zlonamjernih datoteka u karantenu te mogućnost njihova povrata. Naručitelj je navedeno, imajući u vidu funkcionalno formuliran zahtjev dokumentacije o nabavi, ocijenio dostatnim za ispunjenje zahtjeva koji se odnosi na mehanizme zaštite i povrata datoteka u slučaju ransomware aktivnosti.

Naručitelj dalje ističe da je u dijelu točke 3.3. pod f. traženo filtriranje i blokiranje pristupa malicioznim internet domenama izravno na razini hipervizora. Prije prikaza dostavljenih dokaza, naručitelj napominje da dokumentacijom o nabavi nije bilo propisano da funkcionalnost mora biti ostvarena isključivo kroz jednu komponentu ili integrirana unutar ponuđenog rješenja, niti je bila propisana tehnologija kojom se filtriranje i blokiranje pristupa malicioznim internet domenama izravno na razini hipervizora mora provesti. Nadalje, ističe da dokazivanje predmetne funkcionalnosti nije bilo propisano dokumentom Funkcijska podloga. Iako za navedenu funkcionalnost nije bila propisana obveza dokazivanja, naručitelj ukazuje da je prilikom postupka pregleda i ocjene ponuda, radi cjelovitog utvrđenja ispunjenja svih traženih zahtjeva, uzeo u obzir dostavljenu tehničku dokumentaciju i utvrdio je da je odabrani ponuditelj u svojoj ponudi dostavio sljedeće:

- Dokument „CortexXDR_dokumentacija.pdf“, u kojem je na stranici 682. navedena funkcionalnost „Network packet inspection engine“, za koju je opisano da analizira mrežne pakete radi detekcije zlonamjernog ponašanja na mrežnoj razini. Time je po mišljenju naručitelja potvrđeno da ponuđeno rješenje ima mogućnost mrežne analize i detekcije zlonamjernog ponašanja. Slijedom navedenog, naručitelj je, polazeći od funkcionalnog načina na koji je predmetni zahtjev propisao, ocijenio da dostavljena dokumentacija potvrđuje mogućnost mrežne analize, detekcije i blokiranja zlonamjernih komunikacija, dok eventualna potreba integracije s drugim sigurnosnim ili virtualizacijskim komponentama, kao što to navodi žalitelj, predstavlja obvezu odabranog ponuditelja u okviru zahtjeva isporuke sustava do pune funkcionalnosti, bez dodatnih troškova za naručitelja.

U očitovanju na naručiteljev odgovor na žalbu, žalitelj uvodno ističe da ne osporava u formalnom smislu naručiteljevu tvrdnju da zahtjevi opisani slovima a do h iz točke 3.3. Tehničke podloge nisu bili predmet obveznog dokazivanja u dokumentu Funkcijska podloga. Međutim, žalitelj smatra da iz nje ne slijedi da naručitelj može prihvatiti ponudu koja ne ispunjava te zahtjeve, već isključivo da je naručitelj slobodan birati način njihovog verificiranja. Ukazuje da je naručitelj, prema vlastitim navodima, verificirao zahtjeve propisane pod slovima a do h na temelju tehničke dokumentacije odabranog ponuditelja.

Konkretno, žalitelj osporava navod naručitelja prema kojem funkcionalnost „Restore File”, odnosno vraćanje datoteke iz karantene predstavlja ispunjenje zahtjeva za „povratom datoteka”, odnosno ekvivalent funkcionalnosti oporavka podataka. Naručitelj pritom navodi da Funkcijska podloga nije propisivala da ponuđeno rješenje mora sadržavati zaseban backup sustav, već isključivo mogućnost povrata datoteka, te zaključuje da funkcionalnost vraćanja datoteka iz karantene predstavlja dostatno ispunjenje tog zahtjeva. Takvo tumačenje je po mišljenju žalitelja tehnički i funkcionalno pogrešno, jer se radi o dvjema bitno različitim kategorijama funkcionalnosti. Tehnička podloga, u točki 3.3., pod slovom d za licence s uključenom naprednom zaštitom propisuje zahtjev za naprednim mehanizmom detekcije ransomwarea uz automatsko kreiranje backup kopija datoteka povrata. Žalitelj smatra da je zahtjev jezično i tehnički jasan, naime, uz mehanizam detekcije ransomwarea,

ponuđeno rješenje mora automatski kreirati backup kopije (sigurnosne kopije) datoteka, čime se omogućuje njihov povrat u slučaju enkripcije. Radi se o proaktivnoj zaštiti podataka. Funkcionalnost „Restore File”, odnosno vraćanje datoteke iz karantene u sklopu rješenja odabranog ponuditelja, predstavlja mehanizam reaktivnog oporavka datoteka koje su prethodno već identificirane kao potencijalno zlonamjerne te izolirane u karantenu. Osnovna svrha takvog mehanizma je sigurnosna izolacija i kontrolirano vraćanje već postojećih datoteka. Dakle, to je reaktivna operacija koja pretpostavlja da je ransomware već identificiran i zaustavljen, da je datoteka već stavljena u karantenu (tj. premještena i izolirana od ostalih podataka), da administrator ručno ili putem API sučelja inicira povrat te specifične datoteke.

Žalitelj dalje pojašnjava da, nasuprot tome, backup sustav predstavlja preventivni mehanizam zaštite podataka koji podrazumijeva izradu sigurnosnih kopija podataka prije njihovog gubitka, oštećenja ili enkripcije (npr. u slučaju ransomware napada), s ciljem omogućavanja oporavka podataka u stanju prije nastanka sigurnosnog incidenta. Dakle, to je proaktivni mehanizam koji u realnom vremenu, bez intervencije administratora, sprema verziju datoteke, djeluje pri detekciji, dakle prije nego što enkripcija može biti dovršena, omogućuje povrat originalnih, nezašifriranih datoteka čak i ako je enkripcija djelomično uspjela. Slijedom navedenoga, žalitelj zaključuje da se funkcionalnost vraćanja datoteka iz karantene ne može smatrati ekvivalentnom funkcionalnosti backup sustava niti osigurava istu razinu zaštite podataka, budući da ne omogućuje oporavak podataka koji nisu prethodno izolirani u karantenu, niti predstavlja preventivni mehanizam zaštite od gubitka podataka. Prihvaćanje funkcionalnosti "Restore File" kao ispunjenja zahtjeva pod slovom d, po mišljenju žalitelja ne predstavlja samo tumačenje prema kojem nije potreban zaseban backup sustav, već izmjenu same prirode zahtjeva, na način da se proaktivni mehanizam zaštite podataka prihvaća kao reaktivni mehanizam oporavka datoteka. Stoga žalitelj smatra da naručiteljevo tumačenje predstavlja neprihvatljivo izjednačavanje dviju tehnički i funkcionalno različitih kategorija rješenja, čime se opseg zahtjeva naknadno proširuje na način koji nije bio predviđen dokumentacijom o nabavi. Takvo naknadno izjednačavanje funkcionalnosti dovodi do narušavanja načela transparentnosti i jednakog tretmana ponuditelja, budući da se kao dokaz ispunjenja zahtjeva prihvaća funkcionalnost koja objektivno ne ostvaruje istu sigurnosnu svrhu ni razinu zaštite podataka kao zahtijevana funkcionalnost povrata podataka.

Nadalje, žalitelj ukazuje da Tehnička podloga, točka 3.3., pod slovom f propisuje funkcionalnost filtriranja i blokiranja pristupa malicioznim internet domenama izravno na razini hipervizora. Navedeno sadrži dva tehnički precizna pojma koja određuju arhitekturu rješenja "izravno" i "na razini hipervizora", a oba imaju jasno značenje u kontekstu IT sigurnosti. Naime, pojašnjava da zahtjev koji se odnosi na filtriranje „izravno na razini hipervizora” predstavlja precizno definiranu tehničku razinu u virtualizacijskim arhitekturama, pri čemu hipervizor predstavlja sloj virtualizacije koji se nalazi ispod operativnog sustava i omogućuje nadzor i kontrolu virtualnih strojeva neovisno o njihovim razinama operativnih sustava. Takav mehanizam je proaktivan i podrazumijeva zaštitu koja funkcionira neovisno o operacijskom sustavu virtualnih strojeva, nije zaobilaziva od strane zlonamjernog softvera koji kompromitira gostujući OS, ne zahtijeva instalaciju agenta unutar virtualnog stroja, djeluje na razini virtualnog preklopnika, inspektirajući promet prije nego dospije do gostujućeg OS-a.

Žalitelj pojašnjava da nasuprot tome, „network packet inspection engine” na razini operativnog sustava (OS) ili agenta predstavlja funkcionalnost koja djeluje na razini mrežnih paketa unutar operativnog sustava pojedinog virtualnog stroja te je po svojoj prirodi implementirana na višoj razini apstrakcije u odnosu na hipervizorski sloj. Slijedom navedenog, žalitelj ističe da je riječ o dvjema arhitektonski i hijerarhijski različitim razinama

implementacije koje nisu tehnički ekvivalentne niti nužno osiguravaju istu razinu vidljivosti, kontrole i otpornosti na manipulaciju unutar virtualiziranih okruženja. Stoga se zahtjev „na razini hipervizora" ne može tumačiti ekstenzivno kao bilo kakva mrežna inspekcija paketa, već isključivo kao funkcionalnost implementirana na razini virtualizacijskog sloja, kako je i tehnički uobičajeno definirano u industrijskoj praksi virtualizacijskih sigurnosnih rješenja.

Žalitelj ovdje napominje da je uz žalbu priložen specifikacijski list za Palo Alto VM-Series, koji je Palo Alto Networks (proizvođačev) vlastiti proizvod namijenjen upravo zaštiti na razini virtualizacije. Činjenica da Palo Alto Networks za ovu namjenu razvija i prodaje poseban proizvod (VMSeries) koji nije dio Cortex XDR paketa, po mišljenju žalitelja dodatno potvrđuje da Cortex XDR agent ne može ostvariti zahtjev pod slovom f. Konačno, tvrdnja naručitelja prema kojoj je odgovornost odabranog ponuditelja isporuka pune funkcionalnosti bez dodatnih troškova uključujući eventualnu integraciju dodatnih komponenti, po mišljenju žalitelja nije odlučna za ocjenu sukladnosti ponude. Smatra da klauzula o odgovornosti ugovaratelja ne mijenja sadržaj tehničkih zahtjeva propisanih dokumentacijom o nabavi niti ovlašćuje naručitelja da prihvati ponudu koja ih ne ispunjava. Navedena klauzula odnosi se na implementacijske rizike i koordinaciju, a ne na sadržajne tehničke zahtjeve. Žalitelj ističe da bi suprotno tumačenje značilo da naručitelj može prihvatiti i ponudu koja u trenutku predaje ne sadrži traženu funkcionalnost, uz pretpostavku njezine naknadne isporuke, što bi bilo protivno načelu transparentnosti i jednakog tretmana ponuditelja. Osim toga, odabrani ponuditelj u svojoj ponudi nije naveo Palo Alto VM-Series niti bilo koji drugi proizvod koji bi bio kadar ispuniti zahtjev pod točkom f. Žalitelj zaključuje da naručitelj ne može retroaktivno pretpostaviti da će odabrani ponuditelj nabaviti i isporučiti dodatni, neponuđeni proizvod, osobito imajući u vidu da se radi o zasebnom proizvodu s vlastitom tržišnom cijenom.

Naručitelj se očitovao na ove navode žalitelja u podnesku od 27. svibnja 2026. godine na način da ponavlja da dokazivanje funkcionalnosti pod d i f točke 3.3. nije bilo propisano dokumentom Funkcijska podloga, kao i da su zahtjevi bili postavljeni funkcionalno, a ne kroz obvezu primjene točno određenog tehničkog rješenja, tehnologije ili načina provedbe.

Prije ocjene žalbenog navoda treba reći da su odgovarajuće odredbe dokumentacije o nabavi već citirane u rješenju te da stranke ne spore sadržaj podataka iz ponude odabranog ponuditelja koje naručitelj citira i na koje upućuje u odgovoru na žalbu, već oprečno tumače je li tim podacima potvrđeno udovoljavanje uvjetima dokumentacije o nabavi iz točke 3.3. Tehničke podloge pod d i f.

Za ocjenu žalbenog navoda mjerodavne su odredbe članka 280. stavka 4., članka 290. stavka 1. i članka 403. ZJN 2016.

U odnosu na zahtjev iz točke 3.3. pod d, kojim je tražen „napredni mehanizam detekcije ransomwarea uz automatsko kreiranje backup kopija datoteka povrata", Državna komisija prihvaća argumentaciju žalitelja iznesenu u očitovanju na odgovor na žalbu, budući da naručitelj ničime nije dokazao svoju tvrdnju da je funkcionalnost vraćanja datoteka iz karantene („Restore File") tehnički odnosno funkcionalno ekvivalentan zahtijevanom mehanizmu automatskog kreiranja sigurnosnih (backup) kopija datoteka. Naime, žalitelj ističe da se radi o dvjema bitno različitim kategorijama funkcionalnosti, odnosno da zahtjev dokumentacije o nabavi podrazumijeva postojanje proaktivnog mehanizma zaštite podataka, kojim se u trenutku detekcije ransomware aktivnosti automatski kreiraju sigurnosne kopije datoteka radi omogućavanja njihova naknadnog povrata u izvorno stanje. Nasuprot tome, funkcionalnost vraćanja datoteka iz karantene predstavlja reaktivnu radnju koja se odnosi na već identificirane i izolirane datoteke, te ne osigurava kreiranje sigurnosnih kopija prije eventualne enkripcije niti omogućuje oporavak podataka koji nisu prethodno stavljeni u karantenu. Stoga Državna komisija ocjenjuje da se ne može otkloniti

prigovor žalitelja da se navedene funkcionalnosti ne mogu smatrati međusobno ekvivalentnima, niti se funkcionalnost „Restore File“ može prihvatiti kao ispunjenje zahtjeva koji se odnosi na automatsko kreiranje backup kopija datoteka povrata.

U odnosu na zahtjev iz točke 3.3. pod f, kojim je traženo „filtriranje i blokiranje pristupa malicioznim internet domenama izravno na razini hipervizora“, Državna komisija također prihvaća argumentaciju žalitelja da se navedeni zahtjev odnosi na specifičnu arhitektonsku razinu implementacije sigurnosne funkcionalnosti, odnosno na razinu virtualizacijskog sloja (hipervizora), a ne na razinu operativnog sustava ili agentske komponente. Iz podataka na koje se poziva naručitelj proizlazi da ponuđeno rješenje omogućuje mrežnu analizu putem funkcionalnosti „network packet inspection engine“, međutim, kako to ističe žalitelj, takva funkcionalnost djeluje na razini operativnog sustava ili aplikacijskog sloja, odnosno naručitelj nije ničime dokazao da se ista može smatrati ekvivalentnom implementaciji sigurnosne funkcionalnosti izravno na razini hipervizora. Naime, naručitelj nije na uvjerljiv način obrazložio na koji način ponuđeno rješenje ostvaruje zahtijevanu funkcionalnost upravo na toj razini, niti je dostavio podatke iz kojih bi takvo što proizlazilo.

Sukladno pravilima o teretu dokazivanja iz članka 403. ZJN 2016, u situaciji kada žalitelj iznese konkretne i tehnički argumentirane prigovore kojima dovodi u pitanje ispunjenje određenih zahtjeva dokumentacije o nabavi, naručitelj je dužan na jasan i uvjerljiv način otkloniti takve prigovore. U konkretnom slučaju, Državna komisija ocjenjuje da naručitelj nije uspio otkloniti žaliteljeve navode u dijelu koji se odnosi na zahtjeve pod točkama d i f Tehničke podloge. Naime, naručitelj se u očitovanju na žaliteljeve detaljne tehničke prigovore nije sadržajno očitovao, već je ponovio ranije izneseni stav da dokumentacijom o nabavi nije bilo propisano obvezno dokazivanje predmetnih funkcionalnosti kroz Funkcijsku podlogu te da su zahtjevi bili formulirani funkcionalno. Međutim, činjenica da dokumentacijom o nabavi nije bilo propisano formalno dokazivanje pojedinih funkcionalnosti ne znači da naručitelj može prihvatiti ponudu koja objektivno ne udovoljava postavljenim zahtjevima, niti isključuje pravo žalitelja na pravnu zaštitu u odnosu na tvrdnje o neispunjenju tih zahtjeva.

Slijedom navedenog, Državna komisija ocjenjuje da na temelju podataka iz ponude odabranog ponuditelja nije moguće nedvojbeno zaključiti da ponuđeno rješenje udovoljava zahtjevima dokumentacije o nabavi u dijelu koji se odnosi na funkcionalnosti pod točkama d i f Tehničke podloge te se stoga žalbeni navod ocjenjuje osnovanim.

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 postupka javne nabave.

U skladu s prethodno navedenim, na temelju članka 425. stavka 1. točke 4. ZJN 2016 odlučeno je kao u točki 1. izreke ovog rješenja te se predmet vraća naručitelju na ponovno postupanje.

Žalitelj je postavio zahtjev za naknadom troškova žalbenog postupka u iznosu od 1.534,38 eura, koji se sastoji od prethodno plaćene naknade za pokretanje žalbenog postupka i troška prijevoda dokaza po sudskom tumaču.

Članak 431. stavak 2. ZJN 2016. propisuje da Državna komisija odlučuje o troškovima žalbenog postupka, određuje tko snosi troškove žalbenog postupka i njihov iznos te kome se i u kojem roku moraju platiti. Stavak 3. tog članka propisuje da je stranka, na čiju je štetu žalbeni postupak okončan dužna protivnoj stranci nadoknaditi opravdane troškove koji su joj nastali sudjelovanjem u žalbenom postupku. Stavak 6. toga članka,

propisuje da će u slučaju usvajanja žalbe, Državna komisija svojom odlukom naložiti naručitelju plaćanje troškova žalbenog postupka žalitelju u roku od osam dana od dana primitka odluke Državne komisije.

S obzirom na to da je žalbeni zahtjev kojim je traženo poništenje odluke o odabiru osnovan, osnovan je i žaliteljev zahtjev za naknadom troškova žalbenog postupka. Žalitelj ima pravo na naknadu troškova žalbenog postupka u iznosu od 1.320,00 eura, koji iznos je pravilnom primjenom odredaba članka 430.a stavka 1. točke 1. ZJN 2016 prethodno uplatio na ime naknade za pokretanje žalbenog postupka.

Također, ima pravo na naknadu troška koji mu je nastao zbog usluge prijevoda dokaza dostavljenih uz žalbu po ovlaštenom sudskom tumaču, za što je dostavio račun na iznos od 214,38 eura. Stoga je i taj iznos opravdani trošak koji je žalitelju nastao sudjelovanjem u žalbenom postupku te žalitelj ima pravo da mu se naknade troškovi u ukupnom iznosu od 1.534,38 eura.

Slijedom navedenog, odlučeno je kao u točki 2. izreke ovog 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.

ZAMJENICA PREDSJEDNICE

Danijela Antolković

DANIJELA ANTOLKOVIĆ
HR-82400519814

Elektronički potpisano: 02.07.2026T12:57:16 (UTC:2026-07-02T10:57:16Z)
Provjera: https://epotpis.rdd.hr/provjera
Broj zapisa: 2c6eb9f3-004c-402d-bb43-a5796b8560d3