



ÚRAD PRE VEREJNÉ OBSTARÁVANIE

Sekcia dohľadu

Ružová dolina 10, 821 09 Bratislava

Bratislava 05. 01. 2026

Číslo: 15418-6000/2025

Úrad pre verejné obstarávanie ako ústredný orgán štátnej správy pre verejné obstarávanie podľa § 140 a orgán príslušný podľa § 147 písm. c), § 167 ods. 2 písm. b), § 169 ods. 1 písm. b) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov vo veci námietok uchádzača XY (ďalej len „navrhovateľ“) smerujúcich podľa § 170 ods. 3 písm. f) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov proti vyhodnoteniu ponúk vo verejnej súťaži na predmet nadlimitnej zákazky s názvom „Služby podpory prevádzky a rozvoja diela Register a identifikátor právnických osôb a podnikateľov“, vyhlásenej verejným obstarávateľom **Štatistický úrad Slovenskej republiky**, Lamačská cesta 3/C, 840 05 Bratislava – mestská časť Karlova Ves, IČO: 00 166 197 (ďalej len „kontrolovaný“), v Úradnom vestníku Európskej únie č. S 184/2024 dňa 20. 09. 2024 pod značkou 565250-2024 a vo Vestníku verejného obstarávania č. 188/2024 dňa 23. 09. 2024 pod značkou 23445-MSS (ďalej len „verejné obstarávanie“), vydáva toto

r o z h o d n u t i e :

Úrad pre verejné obstarávanie podľa § 175 ods. 1 písm. a) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov **nariaduje kontrolovanému Štatistický úrad Slovenskej republiky**, Lamačská cesta 3/C, 840 05 Bratislava – mestská časť Karlova Ves, IČO: 00 166 197, vo verejnom obstarávaní na predmet nadlimitnej zákazky s názvom „Služby podpory prevádzky a rozvoja diela Register a identifikátor právnických osôb a podnikateľov“, vyhlásenej v Úradnom vestníku Európskej únie č. S 184/2024 dňa 20. 09. 2024 pod značkou 565250-2024 a vo Vestníku verejného obstarávania č. 188/2024 dňa 23. 09. 2024 pod značkou 23445-MSS, **odstrániť protiprávny stav**, a to konkrétne zrušiť Oznámenie o výsledku vyhodnotenia ponúk zo dňa 26. 11. 2025 vrátane aktualizovanej Prílohy č. 1 k Oznámeniu o výsledku vyhodnotenia ponúk odoslanej dňa 01. 12. 2025 a Informáciu o výsledku vyhodnotenia ponúk a poradie uchádzačov zverejnenú na profile kontrolovaného dňa 26. 11. 2025, a opätovne vyhodnotiť u úspešného uchádzača XX podmienku účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému odborníkovi č. 6 - Špecialista na bezpečnosť v súlade s právnym posúdením úradu v bodoch 81 až 83 tohto rozhodnutia, a to do 60 dní odo dňa nadobudnutia právoplatnosti tohto rozhodnutia.

O d ô v o d n e n i e :

1. Navrhovateľ doručil Úradu pre verejné obstarávanie (ďalej len „úrad“) dňa 08. 12. 2025 námietky v elektronickej podobe podľa osobitného predpisu¹ smerujúce podľa § 170 ods. 3 písm. f) zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“) proti vyhodnoteniu ponúk (ďalej len „námietky“). Kontrolovanému boli doručené námietky

¹ Podľa zákona č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente) v znení neskorších predpisov.

navrhovateľa toho istého dňa funkcionalitou informačného systému Josephine (ďalej len „IS Josephine“), prostredníctvom ktorého sa verejné obstarávanie realizuje.

2. Úrad uvádza, že námietky navrhovateľa boli doručené úradu a kontrolovanému v lehote podľa § 170 ods. 4 a v podobe podľa § 170 ods. 9 a obsahujú všetky náležitosti podľa § 170 ods. 5 zákona o verejnom obstarávaní. Navrhovateľ doručil úradu námietky v zmysle § 170 ods. 1 písm. a) zákona o verejnom obstarávaní ako uchádzač. Podľa § 2 ods. 5 písm. c) zákona o verejnom obstarávaní, na účely tohto zákona sa rozumie uchádzačom hospodársky subjekt, ktorý predložil ponuku. Navrhovateľ predložil ponuku dňa 06. 03. 2025 o 09:50:35 hod. V danom prípade má úrad za to, že navrhovateľ preukázal aktívnu vecnú legitimáciu na podanie námietok.
3. Podľa § 172 ods. 1 zákona o verejnom obstarávaní s podaním námietok je navrhovateľ povinný zložiť na účet úradu kauciu. Kaucia musí byť pripísaná na účet úradu najneskôr na druhý pracovný deň nasledujúci po doručení námietok v lehote podľa § 170 ods. 4. Za každú skutočnosť, proti ktorej námietky podľa § 170 ods. 3 smerujú, sa skladá samostatná kaucia.
4. Podľa § 172 ods. 2 zákona o verejnom obstarávaní výška kaucie pri podaní námietok je 0,1 % z predpokladanej hodnoty zákazky alebo koncesie, najmenej však 2 000 eur a najviac
 - a) 10 000 EUR, ak ide o námietky podľa § 170 ods. 3 písm. a) a b),
 - b) 50 000 EUR, ak ide o iné námietky, ako uvedené v písmene a).
5. Podľa ustanovenia § 172 ods. 2 písm. b) zákona o verejnom obstarávaní je výška kaucie pri podaní námietok 0,1 % z predpokladanej hodnoty zákazky alebo koncesie, najmenej však 2000 eur a najviac 50 000 eur, ak ide o iné námietky, ako uvedené v písmene a). Vzhľadom na predpokladanú hodnotu zákazky vo výške 6 481 564,69 EUR bez DPH bol navrhovateľ v danom prípade povinný s podaním námietok zložiť na účet úradu kauciu vo výške 6 481,56 EUR.
6. Úrad lustráciou účtu úradu zistil, že navrhovateľ s podaním námietok zložil na účet úradu dňa 04. 12. 2025 kauciu vo výške 6 481,56 EUR.
7. Na základe vyššie uvedených skutočností má úrad za to, že s podaním námietok navrhovateľa boli splnené procesné podmienky pre konanie vo veci.

Námietky navrhovateľa

8. Navrhovateľ úvodom popisuje celý priebeh predmetného verejného obstarávania, a to počnúc dňom 26. 06. 2025, kedy kontrolovaný zverejnil vo svojom profile prvotný dokument s názvom „Informácia o výsledku vyhodnotenia ponúk“ a navrhovateľovi zaslal „Oznámenie o výsledku XY“ a „Prílohu č. 1 Oznámenia o výsledku XY“ až po vydanie rozhodnutia úradu č. 11915-6000/2025 zo dňa 29. 09. 2025. Navrhovateľ následne konštatuje, že dňa 26. 11. 2025 zaslal kontrolovaný navrhovateľovi dokument „Oznámenie o výsledku 26 11 2025“ a dokument „Oznámenie o výsledku 26 11 2025 príloha 1“ (ďalej len ako „Oznámenie o výsledku vyhodnotenia ponúk“) a dňa 01. 12. 2025 aktualizovaný dokument „Príloha č. 1 Oznámenie o výsledku“ (ďalej len „Príloha č. 1 Oznámenia o výsledku vyhodnotenia ponúk“), pričom v texte správy uviedol, že Príloha č. 1 k Oznámeniu o výsledku vyhodnotenia ponúk zo dňa 26. 11. 2025 nebola aktuálna a že tento dokument predstavuje aktualizovanú verziu predmetnej

Prílohy č. 1. Z uvedených dokumentov navrhovateľ získal prístup k informáciám, že úspešným uchádzačom v postupe zadávania zákazky sa stal XX (ďalej aj ako „úspešný uchádzač“).

9. Navrhovateľ poukazuje na rozhodnutie úradu č. 11915-6000/2025 zo dňa 29. 09. 2025, pričom konštatuje, že kontrolovaný ignoroval závery vyjadrené úradom v predmetnom rozhodnutí úradu a
- nepristúpil k vylúčeniu úspešného uchádzača z dôvodu, že tento uchádzač nepostupoval v súlade so žiadosťou kontrolovaného a nenahradil navrhovaného odborníka č. 6 Špecialista pre bezpečnosť, ktorý nespĺňa požadovanú odbornosť v podobe požadovaných certifikátov,
 - napriek jednoznačným záverom uvedeným v rozhodnutí úradu č. 11915-6000/2025 zo dňa 29. 09. 2025 o nemožnosti prihladiť, resp. vyhodnocovať dodatočne (po uplynutí lehoty na predkladanie ponúk) predložené doklady/certifikáty, opätovne pristúpil k vyhodnoteniu týchto certifikátov,
 - tieto vyhodnotil ako spĺňajúce stanovenú minimálnu požadovanú úroveň štandardov,
 - v Prílohe č. 1 Oznámenia o výsledku vyhodnotenia ponúk len zopakoval rovnaké odôvodnenie, prečo tieto úspešným uchádzačom dodatočne predložené certifikáty spĺňajú stanovenú minimálnu požadovanú úroveň štandardov,
 - s výnimkou, že na poslednej strane Prílohy č. 1 Oznámenia o výsledku vyhodnotenia ponúk (táto strana predstavuje jediný rozdiel oproti verzii tejto prílohy, proti obsahu/výsledkom ktorej navrhovateľ podal námietky dňa 29. 08. 2025), kontrolovaný len stroho spomína znalecký posudok, o ktorom navrhovateľ predpokladá, že si dal kontrolovaný vyhotoviť, pričom o ňom neuvádza absolútne žiadne informácie alebo jeho závery, ktorými sa komisia riadila a na základe ktorých komisia zmenila svoje rozhodnutie o vyhodnocovaní iných certifikátov ako certifikátov, ktoré boli uvedené v Prílohe č. 1 Oznámenia o výsledku vyhodnotenia ponúk zo dňa 26. 11. 2025.
10. Takýto postup podľa navrhovateľa postráda akékoľvek znaky transparentného, nediskriminačného a rovnako zaobchádzajúceho konania zo strany kontrolovaného a smeruje k účelovému výberu uchádzača XX ako úspešného napriek tomu, že tento nespĺňa stanovenú minimálnu požadovanú úroveň štandardov podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní.
11. Navrhovateľ v 1. časti svojich námietok týkajúcej sa požiadavky na platný certifikát CCSP (Certified Cloud Security Professional) pre kľúčového odborníka „Špecialista na bezpečnosť“ uvádza, že kontrolovaný v časti 2. „Technická spôsobilosť alebo odborná spôsobilosť“, v bode 2.5 súťažných podkladov stanovil vo vzťahu k požadovanému kľúčovému odborníkovi - Špecialista na bezpečnosť okrem iných nasledovnú minimálnu požiadavku odbornej praxe a odbornej kvalifikácie, cit.: *„platný certifikát pre CCSP (Certified Cloud Security Professional), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením*

požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač).“

12. Z Prílohy č. 1 Oznámenia o výsledku vyhodnotenia ponúk vyplýva, že úspešný uchádzač na preukázanie splnenia podmienky účasti na disponovanie s certifikátom pre CCSP (Certified Cloud Security Professional) predložil k požadovanému kľúčovému odborníkovi „Špecialista na bezpečnosť“ nasledovný certifikát navrhovaného kľúčového odborníka XXX:

• platný certifikát pre CCSP (Certified Cloud Security Professional), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);	Predložený certifikát a jeho úradný preklad za [REDACTED] [REDACTED] Certifikát: Certified Cloud Security Professional Dátum ukončenia platnosti: 31.07.2028 (dátum začatia platnosti je 14.07.2025) Vydaný spoločnosťou: International Information System Security Certification Consortium
---	--

13. Vo vzťahu k začiatku platnosti uvedeného predloženého certifikátu kontrolovaný v Oznámení o výsledku vyhodnotenia ponúk uviedol, cit.: „Dátum platnosti certifikátov CCSP a CSSLP overovala komisia na webovej stránke: <https://my.isc2.org/s/MemberVerification>, kde dátum začatia platnosti certifikátu CCSP bol 14.07.2025 a certifikátu CSSLP bol 03.03.2025. Komisia vzala do úvahy, že vydanie certifikátov trvá určité časové obdobie, a preto sa priklonila k začatiu platnosti certifikátov so skorším dátumom – t. j. s dátumom, ktorý bol uvedený na webovej stránke: <https://my.isc2.org/s/MemberVerification> a ktorý je zároveň dátumom zloženia skúšky.

Na základe predložených certifikátov CCSP a CSSLP, ich obsahovej analýzy, preukázanej odbornej praxe a dostupných dôkazov komisia vyhodnotila tieto certifikáty ako obsahovo potvrdzujúce odbornú spôsobilosť požadovanú pre kľúčového odborníka - Špecialista na bezpečnosť. Komisia skonštatovala, že predloženými certifikátmi CCSP a CSSLP nejde o dodatočné nadobudnutie kvalifikácie, ale o objasnenie a potvrdenie stavu, ktorý existoval už k dátumu predkladania ponúk.“

14. Navrhovateľ uvádza, že ide o doklad, ktorý kontrolovaný ani nemal vyhodnocovať, keďže mal prístup k vylúčeniu úspešného uchádzača z dôvodu, že v súlade so žiadosťou kontrolovaného nenahradil navrhovaného kľúčového odborníka XXX.
15. Navrhovateľ opätovne poukazuje na skutočnosť, ktorá vyplýva zo záverov rozhodnutia úradu č. [11915-6000/2025](#) zo dňa 29. 09. 2025 a to, že kontrolovaný žiadnym spôsobom nereflektoval na to, že úspešný uchádzač, v reakcii na žiadosť kontrolovaného nenahradil navrhovaného kľúčového odborníka „Špecialista na bezpečnosť“ – XXX, ale predložil nové doklady za túto istú osobu, pričom išlo o doklady, ktoré absentovali v ponuke tohto uchádzača.
16. Navrhovateľ v tejto súvislosti poukazuje na ustálenú rozhodovaciu prax Súdneho dvora EÚ premietnutú do rozhodovacej a metodologickej praxe úradu, v zmysle ktorej nie je v procese vyhodnocovania podmienok účasti možné akceptovať nové doklady, ktoré neboli predložené

v pôvodnej ponuke uchádzača. Tento záver korešponduje s ustálenou judikatúrou Súdneho dvora EÚ, spomedzi ktorej navrhovateľ uvádza rozsudok zo 7. apríla 2016, Partner Apelski Dariusz, C-324/14, EU:C:2016:214, bod 61, 63, 64 a 65.

17. Navrhovateľ uvádza, že tieto závery úrad jednoznačne zhmotnil do poznámky č. 5 v bode 84 rozhodnutia úradu č. 11915-6000/2025 zo dňa 29. 09. 2025, kde uvádza, cit.: *„Úrad dáva do pozornosti, že nenahradenie inej osoby na základe výzvy podľa § 40 ods. 5 zákona o verejnom obstarávaní takou inou osobou, ktorá spĺňa stanovené požiadavky, zakladá dôvod vylúčenia uchádzača podľa § 40 ods. 6 písm. j) tohto zákona, a teda verejný obstarávateľ je povinný vylúčiť z procesu verejného obstarávania uchádzača, ktorého podľa § 40 ods. 5 zákona o verejnom obstarávaní vyzval na nahradenie inej osoby.“*
18. Navrhovateľ preto konštatuje, že kontrolovaný postupoval v rozpore s ustálenou rozhodovacou súdnou praxou a praxou úradu, a zároveň s bezprostredne predchádzajúcim rozhodnutím úradu č. 11915-6000/2025 zo dňa 29. 09. 2025, keď úspešného uchádzača nevylúčil, ale opätovne vyhodnotil a akceptoval dodatočne predložený certifikát CCSP (Certified Cloud Security Professional), ktorý absentoval v jeho ponuke.
19. Navrhovateľ uvádza, že ide o certifikát predložený po lehote na predkladanie ponúk. Zo skutkového stavu sumarizovaného v bodoch 61, 63 a 64 rozhodnutia č. 11915-6000/2025 zo dňa 29. 09. 2025 vyplýva, že:
 - a) lehota na predkladanie ponúk uplynula dňa 06. 03. 2025
 - b) kontrolovaný doručil úspešnému uchádzačovi „Žiadosť o nahradenie osôb určených na plnenie zmluvy“ dňa 25. 07. 2025
 - c) úspešný uchádzač doručil tento certifikát ako odpoveď na uvedenú žiadosť dňa 30. 07. 2025
 - d) dátum začatia platnosti certifikátu je 14. 07. 2025, teda viac ako 4 mesiace po uplynutí lehoty na predkladanie ponúk.
20. Navrhovateľ tvrdí, že uvedené bezpochyby preukazuje znenie pôvodného Oznámenia o výsledku vyhodnotenia ponúk, resp. jeho prílohy, v ktorom sa uvádza, že úspešný uchádzač na preukázanie splnenia minimálnej požadovanej úrovne štandardov viažucej sa ku kľúčovému odborníkovi č. 6 „Špecialista na bezpečnosť“ predložil certifikát Certificate of Cloud Security Knowledge v5. Tento certifikát kontrolovaný pôvodne určil ako spĺňajúci minimálnu požadovanú úroveň štandardov s nasledovným odôvodnením:

uchádzač).	Predložený certifikát a jeho úradný preklad za [REDACTED]
• platný certifikát pre CCSP (Certified Cloud Security Professional), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);	Certifikát: Certificate of Cloud Security Knowledge v5 Dátum vydania: 22.01.2025 Vydaný spoločnosťou: Cloud Security Alliance Certifikát platí na neurčito, bez automatickej expirácie. Predložený certifikát komisia vyhodnotila ako ekvivalent požadovaného certifikátu spĺňajúci podmienku účasti určenú verejným obstarávateľom. Certifikát vydaný Cloud Security Alliance (CSA) je medzinárodne uznávaný certifikát a pokrýva komplexne oblasti bezpečnosti cloudových riešení v rovnakých znalostných doménach ako CCSP.

21. V pôvodnej prílohe Oznámenia o výsledku vyhodnotenia ponúk sa certifikát CCSP na žiadnom mieste neuvádza. Navrhovateľ považuje za nepochybné, že úspešný uchádzač predložil certifikát CCSP (Certified Cloud Security Professional) až dňa 30. 07. 2025, t. j. s výrazným časovým odstupom po uplynutí lehoty na predkladanie ponúk.
22. Navrhovateľ konštatuje, že ide o certifikát vydaný dňa 14. 07. 2025, t. j. viac ako 4 mesiace po uplynutí lehoty na predkladanie ponúk, na certifikačné obdobie od 1. augusta 2025 – 31. júla 2028. Navrhovateľ opätovne poukazuje na vyššie citovanú požiadavku týkajúcu sa certifikátu CCSP, v zmysle ktorej kontrolovaný jednoznačne požadoval predloženie platného certifikátu (alebo ekvivalentu) vydaného medzinárodne uznávanou akreditovanou (certifikovanou) autoritou. Navyše, sám kontrolovaný na viacerých miestach prílohy oznámenia o výsledku vyhodnotenia ponúk uvádza, že dátum začatia platnosti certifikátu CCSP bol 14. 07. 2025 a certifikátu CSSLP, čo si komisia overovala na webovej stránke: <https://my.isc2.org/s/MemberVerification>. Zároveň, ako vyplýva z bodu 64 rozhodnutia č. 11915-6000/2025 zo dňa 29. 09. 2025, úspešný uchádzač predložil certifikát CCSP (Certified Cloud Security Professional) udelený XXX (č. 1860697) na certifikačné obdobie: 1. augusta 2025 – 31. júla 2028.
23. Navrhovateľ uvádza, že kontrolovaný v súťažných podkladoch nestanovil možnosť záujemcom a uchádzačom predložiť len potvrdenie o vykonaní skúšky a definoval požiadavku na predloženie výlučne platného certifikátu, resp. platného vydaného certifikátu alebo jeho platného (vydaného) ekvivalentu. V prípade pripustenia potvrdenia o vykonaní skúšky mal kontrolovaný v súťažných podkladoch v časti týkajúcej sa tejto podmienky účasti uviesť, že bude akceptovať „platný certifikát alebo doklad o vykonaní skúšky na získanie certifikátu“, čo však na žiadnom mieste súťažných podkladov nespravil a zároveň to žiadnym spôsobom zo súťažných podkladov nevyplýva.
24. Podľa rozhodnutia úradu č. 6420-6000/2022-OD zo dňa 01. 06. 2022, cit: „Úrad rovnako uvádza, že uchádzači, teda aj navrhovateľ, musia spĺňať všetky podmienky účasti už v čase predkladania ponuky a musia ich spĺňať počas celého priebehu verejného obstarávania. Bez ohľadu na skutočnosť v akej etape vyhodnocovania ponúk sa verejné obstarávanie nachádza, navrhovateľ musí spĺňať tak podmienky účasti, ako aj požiadavky na predmet zákazky počas celého priebehu verejného obstarávania a túto skutočnosť musí preukázať dokumentami predloženými v rámci ponuky, resp. to musí vedieť preukázať na požiadanie kontrolovaného.“

25. Navrhovateľ má za to, že úspešný uchádzač bol povinný spĺňať stanovenú minimálnu požadovanú úroveň štandardov viažucu sa ku kľúčovému odborníkovi č. 6 „Špecialista na bezpečnosť“, t. j. mal disponovať kľúčovým odborníkom s platným vydaným certifikátom CCSP alebo jeho vydaným ekvivalentom najneskôr k momentu uplynutia lehoty na predkladanie ponúk. Napriek tomu, že ním navrhovaný kľúčový odborník XXX takýmto vydaným certifikátom nedisponuje, resp. ku dňu predloženia ponuky úspešného uchádzača nedisponoval, kontrolovaný v Prílohe č. 1 Oznámenia o výsledku vyhodnotenia ponúk uviedol, že úspešný uchádzač predmetnú podmienku účasti preukázal.
26. Navrhovateľ poukazuje na záver rozsudku Krajského súdu v Bratislave, sp. zn. 5S/3/2015- 489, cit.: *„Teda nadobudnutie znalosti daných systémov na požadovanej úrovni vyjadrenej stanovenou percentuálnou úspešnosťou preukazuje až certifikát vydaný po úspešnom absolvovaní skúšky.“* Navrhovateľ priznáva, že skutkový stav, z ktorého vychádza tento rozsudok nie je totožný – týkal sa certifikácie Oracle, avšak uvedený záver je v plnej miere možné aplikovať na podľa navrhovateľa nezákonný postup vyhodnocovania predloženého certifikátu kľúčového odborníka XXX zo strany kontrolovaného.
27. Navrhovateľ preto konštatuje, že postup komisie, ktorá cit.: *„sa priklonila k začatiu platnosti certifikátov so skorším dátumom – t.j. s dátumom, ktorý bol uvedený na webovej stránke: <https://my.isc2.org/s/MemberVerification> a ktorý je zároveň dátumom zloženia skúšky“* je účelový, nezákonný a v rozpore so znením stanovenej minimálnej požadovanej úrovne štandardov ku kľúčovému odborníkovi č. 6 „Špecialista na bezpečnosť“.
28. Citovaný záver je ako celok v rozpore s predchádzajúcou vetou Prílohy č. 1 Oznámenia o výsledku vyhodnotenia ponúk, a teda: *„Dátum platnosti certifikátov CCSP a CSSLP overovala komisia na webovej stránke: <https://my.isc2.org/s/MemberVerification>, kde dátum začatia platnosti certifikátu CCSP bol 14.07.2025 a certifikátu CSSLP bol 03.03.2025.“*
29. Z uvedeného je zrejmé, že certifikát CCSP mal jasne uvedený dátum platnosti 14. 07. 2025, teda po uplynutí lehoty na predkladanie ponúk, a certifikát CSSLP mal samostatne uvedený dátum začatia platnosti dňa 03. 03. 2025. Rozhodnutie kontrolovaného vzťahovať dátum 03. 03. 2025 aj na platnosť certifikátu CCSP nie je ničím odôvodnená. Podľa názoru navrhovateľa je nepochybné, že certifikát CCSP bol pre kľúčového experta vydaný s platnosťou až od 14. 07. 2025, teda viac ako 4 mesiace po uplynutí lehoty na predkladanie ponúk. Úspešný uchádzač teda ku dňu predkladania ponúk celkom zjavne nespĺňal požiadavku pre kľúčového experta č. 6, a to dispozíciu platným certifikátom CCSP.
30. Navrhovateľ považuje za podstatné uviesť rovnako skutočnosť, že kontrolovaný pri všetkých ostatných požadovaných certifikátoch akceptoval výlučne ich vydané verzie.
31. Navrhovateľ uvádza, že kontrolovaný sa nevysporiadal transparentným spôsobom so závermi rozhodnutia úradu č. 11915-6000/2025 zo dňa 29. 09. 2025. Napriek tomu, že kontrolovaný dňa 01. 12. 2025 doručil navrhovateľovi opravenú Prílohu č. 1 Oznámenia o výsledku vyhodnotenia ponúk, v ktorej sa v absolútnom kontraste s obsahom Prílohy Oznámenia o výsledku vyhodnocovania ponúk zo dňa 26. 11. 2025 uvádza, že kontrolovaný vyhodnotil za spĺňajúce stanovené požiadavky pôvodne v ponuke predložené certifikáty, navrhovateľ poukazuje na účelovosť a netransparentnosť konania kontrolovaného cieleného na výber úspešného uchádzača, ktorý nespĺňa stanovenú podmienku účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní v nasledovnom: Kontrolovaný zaslal dňa 26. 11. 2025

navrhovateľovi Oznámenie o neprijatí ponuky, prílohou ktorého bola Príloha č. 1, ktorá v bode týkajúcom sa certifikátu CCSP kľúčového experta č. 6 uvádza, že úspešný uchádzač predložil k splneniu predmetnej požiadavky Certificate Cloud Security Knowledge v5.

32. Navrhovateľ poukazuje na bod 65 rozhodnutia úradu č. 11915-6000/2025 zo dňa 29. 09. 2025, pričom dodáva, že ak sa kontrolovaný stotožnil so závermi znaleckých posudkov, a teda že certifikát Cloud Security Knowledge v5 nie je ekvivalentný s certifikátom CCSP, nie je možné tvrdiť, že úspešný uchádzač splnil podmienku účasti pre certifikát CCSP predložením certifikátu Cloud Security Knowledge v5. Kontrolovaný teda v Oznámení o výsledku vyhodnotenia ponúk opätovne uvádza, že úspešný uchádzač splnil podmienku účasti predložením neekvivalentného certifikátu.
33. V závere Prílohy č. 1 Oznámenia o výsledku vyhodnotenia ponúk je priložený tzv. „Kontrolný hárok“, v ktorom ale kontrolovaný opätovne uvádza splnenie požiadavky na predloženie certifikátu CCSP doplneným certifikátom CCSP p. XXX, ktorého platnosť začína 14. 07. 2025.
34. Navrhovateľ konštatuje, že uvedené tvrdenia kontrolovaného sú teda vo vzájomnom rozpore (čo je v rozpore so zásadou transparentnosti), pričom nie je možné určiť, ktorý certifikát považuje kontrolovaný za certifikát, ktorý preukazuje splnenie predmetnej podmienky účasti – či je to (i) certifikát Cloud Security Knowledge v5, ktorý preukázateľne nie je ekvivalentným k požadovanému certifikátu CCSP, alebo je to (ii) certifikát CCSP, ktorý bol vydaný po uplynutí lehoty na predkladanie ponúk, a ktorým úspešný uchádzač nedisponoval v čase predloženia ponuky vo verejnom obstarávaní. V každom prípade ani jeden z uvedených certifikátov nepreukazuje splnenie predmetnej požiadavky zákonným spôsobom.
35. Navrhovateľ dodáva, že kontrolovaný ďalej v kontrolnom hárku odkazuje na znalecký posudok, ktorý nie je definovaný ani znalcom či znaleckou organizáciou, ktorá ho vydala, ani jeho číslom ani dátumom vydania. Navrhovateľ teda nemá žiadnu možnosť overiť, či vôbec bol „nejaký“ znalecký posudok k tejto veci zo strany kontrolovaného zabezpečený. Takto uvedené informácie v Prílohe č. 1 Oznámenia o výsledku vyhodnotenia ponúk sú v rozpore s ustanovením § 55 ods. 2 písm. c) zákona o verejnom obstarávaní, Všeobecným metodickým usmernením č. 6-2025 a rovnako aj v rozpore so zásadou transparentnosti verejného obstarávania.
36. K dodatočne predloženému certifikátu CSSLP (Certified Secure Software Lifecycle Professional) navrhovateľ v 2. časti svojich námietok uvádza, že kontrolovaný v časti 2. „Technická spôsobilosť alebo odborná spôsobilosť“, v bode 2.5 súťažných podkladov stanovil vo vzťahu k požadovanému kľúčovému odborníkovi - Špecialista na bezpečnosť okrem iných nasledovnú minimálnu požiadavku odbornej praxe a odbornej kvalifikácie, cit.: *„platný certifikát pre CSSLP (Certified Secure Software Lifecycle Professional, alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač).“*
37. Navrhovateľ konštatuje, že z Prílohy č. 1 Oznámenia o výsledku vyhodnotenia ponúk vyplýva, že úspešný uchádzač na preukázanie splnenia požiadavky na disponovanie s certifikátom pre CSSLP (Certified Secure Software Lifecycle Professional) predložil k požadovanému kľúčovému odborníkovi „Špecialista na bezpečnosť“ nasledovný certifikát navrhovaného kľúčového odborníka XXX:

• platný certifikát pre CSSLP (Certified Secure Software Lifecycle Professional, alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);	Predložený certifikát a jeho úradný preklad za [REDACTED] Certifikát: Certified Secure Software Lifecycle Professional Dátum ukončenia platnosti: 31.03.2028 (dátum začatia platnosti 03.03.2025) Vydaný spoločnosťou: International Information System Security Certification Consortium Dátum platnosti certifikátov CCSP a CSSLP overovala [REDACTED]
--	--

38. Navrhovateľ dodáva, že k vyhodnoteniu (aj) tohto certifikátu kontrolovaný v Prílohe č. 1 Oznámenia o výsledku vyhodnotenia ponúk uviedol, cit.: „Na základe predložených certifikátov CCSP a CSSLP, ich obsahovej analýzy, preukázanej odbornej praxe a dostupných dôkazov komisia vyhodnotila tieto certifikáty ako obsahovo potvrdzujúce odbornú spôsobilosť požadovanú pre kľúčového odborníka – Špecialista na bezpečnosť. Komisia skonštatovala, že predloženými certifikátmi CCSP a CSSLP nejde o dodatočné nadobudnutie kvalifikácie, ale o objasnenie a potvrdenie stavu, ktorý existoval už k dátumu predkladania ponúk.“ S takýmto vyhodnotením, resp. odôvodnením vyhodnotenia sa navrhovateľ rovnako nemôže stotožniť, keďže ide o doklad, ktorý kontrolovaný ani nemal vyhodnocovať, keďže mal pristúpiť k vylúčeniu úspešného uchádzača z dôvodu, že v súlade so žiadosťou kontrolovaného nenahradil navrhovaného kľúčového odborníka XXX.
39. Navrhovateľ konštatuje, že kontrolovaný postupoval v rozpore v ustálenou rozhodovacou súdnou praxou a praxou úradu, a zároveň s bezprostredne predchádzajúcim rozhodnutím úradu č. 11915-6000/2025 zo dňa 29. 09. 2025, keď úspešného uchádzača nevyhlásil, ale opätovne vyhodnotil a akceptoval dodatočne predložený certifikát CSSLP (Certified Secure Software Lifecycle Professional), ktorý absentoval v jeho ponuke.
40. Navrhovateľ konštatuje, že zároveň ide o certifikát predložený po uplynutí lehoty na predkladanie ponúk. Navrhovateľ konštatuje, že úspešný uchádzač doručil tento certifikát ako odpoveď na uvedenú žiadosť dňa 30. 07. 2025.
41. Uvedené podľa názoru navrhovateľa bezpochyby preukazuje znenie pôvodného Oznámenia o výsledku vyhodnotenia ponúk, resp. jeho prílohy, v ktorom sa uvádza, že úspešný uchádzač na preukázanie splnenia minimálnej požadovanej úrovne štandardov viažucej sa ku kľúčovému odborníkovi č. 6 „Špecialista na bezpečnosť“ predložil certifikát CompTIA Security+ Certified CE. Tento certifikát kontrolovaný pôvodne určil ako spĺňajúci minimálnu požadovanú úroveň štandardov s nasledovným odôvodnením:

• platný certifikát pre CSSLP (Certified Secure Software Lifecycle Professional, alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);	Predložený certifikát a jeho úradný preklad za [REDACTED] Certifikát: CompTIA Security+ Certified CE Dátum ukončenia platnosti: 17.10.2027 Vydaný spoločnosťou: CompTia Komisia vyhodnotila predložený certifikát ako spĺňajúci podmienku účasti určenú verejným obstarávateľom, nakoľko certifikát CompTIA Security+ Certified CE je medzinárodne uznávaný bezpečnostný certifikát, ktorý pokrýva základné až stredne pokročilé princípy kybernetickej bezpečnosti, vrátane aspektov bezpečného vývoja softvéru, autentifikácie, šifrovania, riadenia prístupu a bezpečnostných auditov. Aj keď CSSLP je špecializovaný na bezpečnosť v rámci životného cyklu vývoja softvéru (secure SDLC), CompTIA Security+ má širší bezpečnostný záber a je uznávaný ako vstupný až stredne pokročilý certifikát v oblasti IT
	bezpečnosti, vrátane vývoja. Je preto primeranou alternatívou najmä ak bol doplnený praktickou skúsenosťou uchádzača pri vývoji zabezpečených aplikácií. Predložený certifikát CompTIA Security+ spĺňa odborné predpoklady v oblasti bezpečnosti softvéru v primeranom rozsahu, pričom ho možno považovať za dostatočne relevantný a akceptovateľný ekvivalent za CSSLP, najmä vzhľadom na prax odborníka.

42. V pôvodnej prílohe Oznámenia o výsledku vyhodnotenia ponúk sa certifikát CSSLP na žiadnom mieste neuvádza. Navrhovateľ považuje za nepochybné, že úspešný uchádzač predložil certifikát CSSLP (Certified Secure Software Lifecycle Professional) dňa 30. 07. 2025, t. j. s výrazným časovým odstupom po uplynutí lehoty na predkladanie ponúk.
43. Navrhovateľ v 3. časti svojich námietok uvádza, že predložený certifikát Certified GRC Professional (GRCP) nepredstavuje ekvivalent požadovaného certifikátu CGRC (Certified Governance, Risk and Compliance).
44. Navrhovateľ uvádza, že kontrolovaný v časti 2. „Technická spôsobilosť alebo odborná spôsobilosť“, v bode 2.5 súťažných podkladov stanovil vo vzťahu k požadovanému kľúčovému odborníkovi - Špecialista na bezpečnosť okrem iných nasledovnú minimálnu požiadavku odbornej praxe a odbornej kvalifikácie, cit.: „*platný certifikát pre CGRC (Certified Governance, Risk and Compliance), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač).*“
45. Navrhovateľ tvrdí, že z Oznámenia o výsledku vyhodnotenia ponúk vyplýva, že úspešný uchádzač na preukázanie splnenia požiadavky na disponovanie s certifikátom pre CGRC (Certified Governance, Risk and Compliance), predložil k požadovanému kľúčovému

odborníkovi „Špecialista na bezpečnosť“ nasledovný certifikát navrhovaného kľúčového odborníka XXX:

• platný certifikát pre CGRC (Certified Governance, Risk and Compliance), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);	Predložený certifikát a jeho úradný preklad za [REDACTED] Certifikát: Certified GRC Profesional (GRCP) Dátum ukončenia platnosti: 26.01.2026 Vydaný spoločnosťou: OCEG and GRC Certify
---	---

46. Navrhovateľ opätovne, rovnako ako v jeho námietkach zo dňa 29. 08. 2025 uvádza, že na základe dôvodných pochybností o správnosti konštatovania kontrolovaného, že úspešným uchádzačom predložený certifikát (uvedeného navrhovaného kľúčového odborníka) predstavuje ekvivalent ku kontrolovaným požadovanému certifikátu, požiadal znaleckú organizáciu Kompetenčné a certifikačné centrum kybernetickej bezpečnosti, so sídlom Na družstvo 125, 91625 Brunovce o vypracovanie znaleckého posudku k ekvivalencii certifikátu pre CGRC (Certified Governance, Risk and Compliance) a certifikátu Certified GRC Professional (GRCP).
47. V súlade so závermi tohto znaleckého posudku navrhovateľ konštatuje, že úspešným uchádzačom predložený certifikát Certified GRC Professional (GRCP) nepredstavuje ekvivalent požadovaného certifikátu CGRC (Certified Governance, Risk and Compliance).
48. Navrhovateľ má za to, že kontrolovaný postupoval v rozpore s § 40 ods. 1 zákona o verejnom obstarávaní, keď nevyhodnotil vyššie uvedené minimálne požiadavky odbornej praxe a odbornej kvalifikácie vo vzťahu ku kľúčovému odborníkovi č. 6 - Špecialista na bezpečnosť v súlade s požiadavkami, ktoré si sám stanovil, tým, že úspešným uchádzačom predložený certifikát Certified GRC Professional (GRCP) uznal ako ekvivalentný k požadovanému certifikátu CGRC (Certified Governance, Risk and Compliance) napriek tomu, že tento ekvivalentným certifikátom nie je.
49. Navrhovateľ konštatuje, že kontrolovaný pri vyhodnotení predložených certifikátov kľúčového odborníka XXX nepostupoval v súlade s minimálnou požadovanou úrovňou štandardov viažucou sa ku kľúčovému odborníkovi č. 6 „Špecialista na bezpečnosť“, ktorú stanovil v súťažných podkladoch, čím porušil svoju povinnosť uvedenú v § 40 ods. 1 zákona o verejnom obstarávaní.
50. Uvedené konanie kontrolovaného zároveň podľa názoru navrhovateľa predstavuje porušenie základných princípov verejného obstarávania podľa § 10 ods. 2 zákona o verejnom obstarávaní, najmä princípov nediskriminácie, rovnakého zaobchádzania s uchádzačmi a transparentnosti, keďže kontrolovaný ním na jednej strane zvýhodnil úspešného uchádzača, keď

- primárne ho nevytlúčil z dôvodu, že v súlade s jeho žiadosťou nenahradil navrhovaného kľúčového odborníka XXX iným navrhovaným kľúčovým odborníkom, ktorý spĺňa stanovenú minimálnu požadovanú úroveň štandardov, ale
- akceptoval certifikát CCSP (Certified Cloud Security Professional) vydaný a predložený po uplynutí lehoty na predkladanie ponúk,
- akceptoval certifikát CSSLP (Certified Secure Software Lifecycle Professional), predložený po uplynutí lehoty na predkladanie ponúk, a zároveň
- akceptoval certifikát Certified GRC Professional (GRCP) napriek tomu, že tento nepredstavuje ekvivalent požadovaného certifikátu CGRC (Certified Governance, Risk and Compliance),

keď úspešného uchádzača zvýhodnil oproti iným uchádzačom a vyhlásil ho za splňajúceho podmienky účasti napriek tomu, že tento preukázateľne nesplnil minimálne požiadavky odbornej praxe a odbornej kvalifikácie u požadovaného kľúčového odborníka č. 6 „Špecialista na bezpečnosť“.

51. Navrhovateľ v tejto súvislosti upriamuje pozornosť na bod 42 rozhodnutia Rady úradu č. 109-9000/2014-KR/2, cit.: *„V súlade s vyššie uvedeným princípom (pozn. transparentnosti) je následne kladená požiadavka na verejného obstarávateľa, aby vyžadované podmienky účasti čisto a prehľadne vyhodnotil v súlade s tým, čo bolo v oznámení o vyhlásení verejného obstarávania stanovené. Teda inak povedané, aby postupoval v súlade s tým, čo si sám stanovil, v žiadnom prípade však už v tejto fáze verejného obstarávania po predložení ponúk nemôže vykladať stanovené podmienky účasti, resp. doklady slúžiace na ich preukázanie, iným spôsobom, meniť ich alebo inak si ich vo svoj prospech alebo v prospech iných hospodárskych subjektov prispôbovať. Tieto jedny zo základných požiadaviek na proces verejného obstarávania je potrebné v každom prípade zo strany verejného obstarávateľa dodržať, nakoľko predstavujú predpoklad na následné dosiahnutie a naplnenie ďalších princípov verejného obstarávania, a to princípu rovnakého zaobchádzania a nediskriminácie, ktorý by iste nebol dodržaný pri takom postupe verejného obstarávania, ktorý nepostupuje pri vyhodnocovaní v súlade so stanovenými podmienkami účasti pri niektorom záujemcovi alebo uchádzačovi, ako aj princípu hospodárnosti a efektívnosti verejného obstarávania, keďže dôsledkom takéhoto postupu verejného obstarávateľa môže byť vylúčenie najvýhodnejšej ponuky alebo ponúk z hľadiska nastavených kritérií.“*
52. Navrhovateľ uvádza, že základné princípy verejného obstarávania majú zabezpečiť voľnú a efektívnu súťaž uchádzačov o zákazky, ktoré sú financované z verejných zdrojov, t. j. prvotný záujem je na efektívnej konkurencii s tým, že záujem na účelnom vynakladaní verejných prostriedkov pristupuje až následne, keď tento cieľ má byť dosiahnutý práve prostredníctvom zabezpečenia nediskriminačného a transparentného zaobchádzania so všetkými dodávateľmi, ktorí sú vzájomnými konkurentmi. Navrhovateľ poukazuje na zásadu rovnakého zaobchádzania a na rozsudok Krajského súdu v Bratislave sp. zn. 2S 123/11-136 a rozsudok Krajského súdu v Bratislave 2S 145/2013 zo dňa 14. 05. 2014.
53. Navrhovateľ tvrdí, že vo výsledku bol v postupe zadávania zákazky za úspešného uchádzača opätovne vyhlásený uchádzač, ktorý predloženými dokladmi nepreukázal splnenie stanovených podmienok účasti, čo nepochybne má zásadný vplyv na výsledok vyhodnotenia ponúk.

54. V súlade s uvedeným navrhovateľ vyjadruje presvedčenie, že opísaný účelový a nezákonný postup kontrolovaného pri vyhodnotení splnenia podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní nemôže požívať právnu ochranu.
55. Navrhovateľ v petite svojich námietok žiada, aby úrad nariadil kontrolovanému v súlade s § 175 ods. 1 písm. a) zákona o verejnom obstarávaní odstrániť protiprávny stav, konkrétne zrušiť výsledok vyhodnotenia ponúk a pokračovať v postupe zadávania zákazky opätovným vyhodnotením ponuky úspešného uchádzača z hľadiska splnenia minimálnej požadovanej úrovne štandardov podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému expertovi č. 6 – Špecialista na bezpečnosť, a to v súlade s rozhodnutím úradu č. 11915-6000/2025 zo dňa 29. 09. 2025.

Začatie preskúmania úkonov kontrolovaného

56. Podľa § 171 ods. 1 zákona o verejnom obstarávaní námietkové konanie sa začína dňom doručenia námietok úradu. Na základe uvedeného úrad konštatuje, že predmetné námietkové konanie sa začalo dňa **08. 12. 2025**.
57. Podľa § 173 ods. 1 písm. a) zákona o verejnom obstarávaní kontrolovaný je povinný doručiť úradu písomné vyjadrenie k podaným námietkam a kompletnú dokumentáciu potrebnú na posúdenie namietaných skutočností, a to do piatich pracovných dní odo dňa doručenia námietok kontrolovanému, ak ide o námietkové konanie; úrad neprihliada na písomné vyjadrenie k podaným námietkam a dôkazy doručené kontrolovaným po uplynutí tejto lehoty.
58. Podľa § 173 ods. 2 zákona o verejnom obstarávaní ak ide o elektronickú komunikáciu, dokumentácia sa úradu doručuje sprístupnením elektronickej podoby dokumentácie zariadením prístupu do elektronického prostriedku použitého na elektronickú komunikáciu v lehote podľa odseku 1, pričom súčasťou elektronickej podoby dokumentácie sú aj auditné záznamy o všetkých úkonoch vykonaných v použitom elektronickej prostriedku. Ak kontrolovaný predkladá dokumentáciu alebo jej časť v listinnej podobe, môže úradu doručiť aj fotokópiu tejto dokumentácie, ak zároveň písomne potvrdí, že táto dokumentácia súhlasí s originálnym vyhotovením dokumentácie. Kontrolovaný môže nahliadať do dokumentácie ním doručenej úradu. Ak sa preskúmanie úkonov kontrolovaného nezačne, úrad bez zbytočného odkladu poskytnutú dokumentáciu vráti.
59. Kontrolovaný dňa 20. 01. 2025 zriadil v prospech úradu prístup k zákazke v IS Josephine v predchádzajúcom konaní o námietkach č. 3816-6000/2025, pričom vyjadrenie k námietkam navrhovateľa podľa § 173 ods. 1 písm. a) zákona o verejnom obstarávaní úradu nedoručil. Na základe uvedeného úrad konštatuje, že dokumentáciu doručенú kontrolovaným v elektronickej podobe potrebnú na posúdenie namietaných skutočností v tomto revíznom konaní považuje za kompletnú odo **dňa začatia konania, t. j. 08. 12. 2025**.

Vyjadrenie kontrolovaného

60. Úrad konštatuje, že kontrolovaný v lehote podľa § 173 ods. 1 písm. a) zákona o verejnom obstarávaní vyjadrenie k námietkam navrhovateľa nedoručil.

Právny rámec

61. Podľa § 10 ods. 1 zákona o verejnom obstarávaní verejný obstarávateľ a obstarávateľ sú povinní pri zadávaní zákaziek, koncesií a pri súťaži návrhov postupovať podľa tohto zákona.
62. Podľa § 10 ods. 2 zákona o verejnom obstarávaní verejný obstarávateľ a obstarávateľ musia dodržať princíp rovnakého zaobchádzania, princíp nediskriminácie hospodárskych subjektov, princíp transparentnosti, princíp proporcionality a princíp hospodárnosti a efektívnosti.
63. Podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní technická spôsobilosť alebo odborná spôsobilosť sa preukazuje podľa druhu, množstva, dôležitosti alebo využitia dodávky tovaru, stavebných prác alebo služieb doloženým jedným alebo niekoľkými z týchto dokladov: ak ide o stavebné práce alebo služby, údajmi o vzdelaní a odbornej praxi alebo o odbornej kvalifikácii osôb určených na plnenie zmluvy alebo koncesnej zmluvy alebo riadiacich zamestnancov, ak nie sú kritériom na vyhodnotenie ponúk.
64. Podľa § 34 ods. 3 zákona o verejnom obstarávaní uchádzač alebo záujemca môže na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti využiť technické a odborné kapacity inej osoby, bez ohľadu na ich právny vzťah. V takomto prípade musí uchádzač alebo záujemca verejnému obstarávateľovi alebo obstarávateľovi preukázať, že pri plnení zmluvy alebo koncesnej zmluvy bude skutočne používať kapacity osoby, ktorej spôsobilosť využíva na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti. Skutočnosť podľa druhej vety preukazuje záujemca alebo uchádzač písomnou zmluvou uzavretou s osobou, ktorej technickými a odbornými kapacitami mieni preukázať svoju technickú spôsobilosť alebo odbornú spôsobilosť. Z písomnej zmluvy musí vyplývať záväzok osoby, že poskytne svoje kapacity počas celého trvania zmluvného vzťahu. Osoba, ktorej kapacity majú byť použité na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti, musí preukázať splnenie podmienok účasti týkajúce sa osobného postavenia a nesmú u nej existovať dôvody na vylúčenie podľa § 40 ods. 6 písm. a) až g) a ods. 7; oprávnenie dodávať tovar, uskutočňovať stavebné práce, alebo poskytovať službu preukazuje vo vzťahu k tej časti predmetu zákazky alebo koncesie, na ktorú boli kapacity záujemcovi alebo uchádzačovi poskytnuté. Ak ide o požiadavku súvisiacu so vzdelaním, odbornou kvalifikáciou alebo relevantnými odbornými skúsenosťami najmä podľa odseku 1 písm. g), uchádzač alebo záujemca môže využiť kapacity inej osoby len, ak táto bude reálne vykonávať stavebné práce alebo služby, na ktoré sa kapacity vyžadujú. Verejný obstarávateľ alebo obstarávateľ môže u osoby, ktorej kapacity majú byť použité na preukázanie technickej spôsobilosti alebo odbornej spôsobilosti, hodnotiť existenciu dôvodov na vylúčenie podľa § 40 ods. 8.
65. Podľa § 40 ods. 5 písm. c) zákona o verejnom obstarávaní verejný obstarávateľ a obstarávateľ sú povinní písomne požiadať uchádzača alebo záujemcu, aby v lehote, ktorá nesmie byť kratšia ako päť pracovných dní odo dňa doručenia žiadosti, nahradil inú osobu, ktorej prostredníctvom preukazuje finančné a ekonomické postavenie alebo technickú spôsobilosť alebo odbornú spôsobilosť, ak existujú dôvody na jej vylúčenie.
66. Podľa § 40 ods. 6 písm. j) zákona o verejnom obstarávaní verejný obstarávateľ a obstarávateľ vylúčia kedykoľvek počas verejného obstarávania uchádzača alebo záujemcu, ak nenahradil inú osobu, prostredníctvom ktorej preukazuje splnenie podmienok účasti finančného a

ekonomického postavenia alebo technickej spôsobilosti alebo odbornej spôsobilosti, ktorá nespĺňa určené požiadavky, v určenej lehote inou osobou, ktorá spĺňa určené požiadavky.

67. Podľa § 175 ods. 1 písm. a) zákona o verejnom obstarávaní ak úrad v preskúmaní úkonov kontrolovaného zistí, že postupom kontrolovaného bol porušený tento zákon a ide o námietkové konanie, rozhodnutím nariadi vo vzťahu k zákazke alebo koncesii alebo ich časti odstrániť protiprávny stav, ak porušenie malo alebo mohlo mať vplyv na výsledok verejného obstarávania.
68. Podľa § 175 ods. 8 zákona o verejnom obstarávaní ak úrad konštatuje porušenie tohto zákona kontrolovaným, v odôvodnení je povinný uviesť aj
- a) všetky zistené porušenia tohto zákona, v rozsahu námietok alebo v rozsahu preskúmania úkonov kontrolovaného v rámci kontroly, ktoré mali alebo mohli mať vplyv na výsledok verejného obstarávania spolu s údajom, či zistené porušenie malo alebo mohlo mať vplyv na výsledok verejného obstarávania a
 - b) stručný návod pre kontrolovaného, ako v druhovo rovnakej veci v budúcnosti predísť porušeniu tohto zákona.

Právne posúdenie úradom

Úrad preskúmal postup kontrolovaného v predmetnom verejnom obstarávaní v rozsahu namietaných skutočností a po zhodnotení všetkých podkladov, najmä dokumentácie predloženej kontrolovaným a navrhovateľom namietaných skutočností konštatuje nasledovné:

69. Úrad uvádza, že v závislosti od predmetu zákazky, typu kontrolovaného a celkovej predpokladanej hodnoty zákazky vo výške 6 481 564,69 eur bez DPH, ide o nadlimitnú zákazku na poskytnutie služieb. Zákazka nie je financovaná z fondov Európskej únie. Kontrolovaný dňa 20. 09. 2024 priamo a bez obmedzení zverejnil súťažné podklady vo svojom profile na webovom sídle úradu. V lehote na predkladanie ponúk, t. j. do 06. 03. 2025 do 10:00, predložili ponuku 3 uchádzači, vrátane navrhovateľa. Po tom, čo kontrolovaný v rámci opätovného vyhodnotenia splnenia podmienok účasti u úspešného uchádzača podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní odoslal dňa 26. 11. 2025 Oznámenie o výsledku vyhodnotenia ponúk a dňa 01. 12. 2025 opravenú Prílohu č. 1 Oznámenia o výsledku vyhodnotenia ponúk, navrhovateľ dňa 08. 12. 2025 doručil úradu a kontrolovanému námietky podľa § 170 ods. 3 písm. f) zákona o verejnom obstarávaní proti vyhodnoteniu ponúk.
70. Úrad uvádza, že kontrolovaný po právoplatnosti rozhodnutia úradu č. [11915-6000/2025](#) zo dňa 29. 09. 2025 (ďalej aj ako „predchádzajúce rozhodnutie“), ktorým úrad nariadil kontrolovanému zrušiť Oznámenie o výsledku vyhodnotenia ponúk zo dňa 20. 08. 2025 a Informáciu o výsledku vyhodnotenia ponúk a poradie uchádzačov zverejnenú na profile kontrolovaného dňa 20. 08. 2025, a opätovne vyhodnotiť u úspešného uchádzača podmienku účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému odborníkovi č. 6 - Špecialista na bezpečnosť, kontrolovaný dňa 17. 11. 2025 adresoval úspešnému uchádzačovi „Výzvu na predloženie dokladov – názov zákazky: Služby podpory prevádzky a rozvoja diela Register a identifikátor právnických osôb a podnikateľov“ zo dňa 13. 11. 2025 (ďalej len „žiadosť o vysvetlenie“), v ktorej je uvedené, cit.: „Verejný obstarávateľ, Štatistický úrad Slovenskej republiky, Vás v zmysle rozhodnutia ÚVO č.: 11915-6000/2025 zo dňa 29. 09. 2025 vyzýva na predloženie dokladov k splneniu podmienky

účasti v zmysle § 34 ods. 1 písm. g) ZVO, nakoľko ÚVO v predmetnom rozhodnutí stanovil opätovne vyhodnotiť u úspešného uchádzača XX podmienku účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému odborníkovi č. 6 – Špecialista na bezpečnosť. (...) Žiadame Vás predložiť všetky doklady preukazujúce splnenie predmetnej podmienky účasti do 5 pracovných dní odo dňa doručenia prostredníctvom IS Josephine. “

71. Úspešný uchádzač dňa 24. 11. 2025 doručil kontrolovanému „Odpoveď na výzvu na predloženie dokladov dňa 17. 11. 2025“ (ďalej len „odpoveď na žiadosť o vysvetlenie“), v ktorej je uvedené, cit.:

„Opätovne Vám predkladáme všetky relevantné dokumenty preukazujúce splnenie podmienky účasti vo vzťahu k ku kľúčovému expertovi č. 6 - Špecialista na bezpečnosť, v našom prípade ku kľúčovému expertovi XXX:

1. Životopis (tak ako už bol predložený) preukazujúci
 - a. dĺžku praxe v stanovenej oblasti, t. j. minimálne šesťdesiat (60) mesiacov odbornej praxe v oblasti kyberbezpečnosti informačných systémov
 - b. požadované praktické skúsenosti, t. j. minimálne dve (2) profesionálne praktické skúsenosti v oblasti kybernetickej bezpečnosti informačných systémov v súlade s bezpečnostnými štandardami podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, alebo ekvivalent v krajine uchádzača, kde hodnota implementovaného informačného systému bola v minimálnej výške 1.000.000 EUR bez DPH
2. Certifikát CISA, ktorý samotný verejný obstarávateľ vydefinoval ako ekvivalent k požadovanému certifikátu RESILIA,
3. Ekvivalentné certifikáty pre oblasť certifikátu CCSP (ekvivalentnosť odôvodňujeme nižšie),
4. Certifikát CSSLP (Certified Secure Software Lifecycle Professional) pre oblasť CSSLP,
5. Certifikát GRC Professional (GRCP) ako ekvivalentný certifikát pre oblasť CGRC (Certified Governance, Risk and Compliance) a
6. Certifikát OMG Certified UML Professional 2 (OCUP 2) ako ekvivalentný certifikát pre oblasť UML 2 Advance Professional.

Ako dôkazy ekvivalentnosti certifikátov predkladáme znalecký posudok, ktorého závermi sú, že

- Certifikát OCUP 2 Advanced (OMG Certified UML Professional 2 - Advanced Level) je plne obsahovo, kvalifikačne aj odborne ekvivalentný certifikátu označenému ako „UML 2 Advanced Professional“,
- Certifikát GRCP (OCEG) je obsahovo ekvivalentný certifikátu CGRC (ISC2). Pokrytie domén governance, risk management a compliance je preukázateľné podľa sylabov oboch certifikácií. Rozdiely sú len v aplikačnom rozsahu (GRCP = širší enterprise GRC, CGRC = IT/IS špecifické riadenie). GRCP je preto plnohodnotný a uznateľný ekvivalent CGRC v kontexte predmetnej zákazky.
- Na základe komplexného posúdenia predložených certifikátov, ich rozsahu, úrovne a uznania znalec konštatuje, že kľúčový odborník navrhovaný uchádzačom preukazuje splnenie požiadavky verejného obstarávateľa na kvalifikáciu pre funkciu Špecialista na bezpečnosť. Predložené certifikácie sú obsahovo a kvalifikačne plne zhodné alebo nadradené požiadavkám uvedeným

v súťažných podkladoch a predstavujú štandardný a medzinárodne akceptovaný dôkaz odbornej spôsobilosti pre výkon špecializovaných úloh v oblasti informačnej a kybernetickej bezpečnosti. Požiadavka na kvalifikáciu kľúčového odborníka - Špecialista na bezpečnosť - je podľa zistení znalca preukázateľne splnená.

Ďalej si dovoľujeme predložiť komparatívnu analýzu ekvivalentnosti skúseností a znalostí uvedeného experta pána XXX ku dňu uplynutia lehoty na predkladanie ponúk vo vzťahu požiadavke verejného obstarávateľa na certifikáciu pre oblasť certifikátu CCSP.

Gap Analýza (rozdielová analýza):

Certifikácia pre oblasť CCSP vs. súbor/kumulácia certifikácií CISA + CSSLP + CGRC + CCSK + CompTIA Security+ + UML2

Gap analýza znamená identifikáciu oblastí, kde je CCSP pokrytý (alebo čiastočne pokrytý) znalosťami z kumulácie, a kde sú medzery (gaps), teda témy, ktoré CCSP vyžaduje, ale kumulácia vyššie uvedeného súboru certifikácií ich neposkytuje v plnom rozsahu.

Metodika Analýzy

- *Zdroje: Založené na oficiálnych syllabách a doménach certifikátov (z overených zdrojov ako ISC , ISACA, Cloud Security Alliance, CompTIA, OMG atď.).*
- *Štruktúra: Porovnanie každej zo 6 domén CCSP (vrátane ich váhy v skúške) s kumuláciou certifikátov. Pre každú doménu uvádzame:*
 - *Pokrytie kumuláciou: Ktoré certifikáty prispievajú a ako.*
 - *Gaps (medzery): čo chýba alebo je nedostatočne pokryté.*
 - *Celkové hodnotenie: Stupeň pokrytia (vysoký, stredný, nízky) a odporúčania.*
- *Predpoklady: Kumulácia znamená kombinované znalosti všetkých certifikátov. CCSP je špecificky zameraný na cloud security, zatiaľ čo kumulácia je širšia (auditing, software security, GRC, general security, modeling), ale menej špecifická pre cloud.*
- *Poznámka: UML2 (OMG Certified UML Professional 2) je zameraný na modelovanie (UML diagramy), čo má minimálny prekryv s security témami, ale môže pomôcť v dizajne architektúry.*

CCSP má celkovo 150 otázok, trvá 4 hodiny, vyžaduje 5 rokov skúseností v IT/security (z toho 3 v cloud security).

Zhrnutie Domén Certifikátov v Kumulácii (pre kontext)

- *CISA: Auditing IT systémov (5 domén: auditing process, governance, acquisition/development, operations/resilience, asset protection).*
- *CSSLP: Secure software lifecycle (8 domén: concepts, lifecycle, requirements, design, implementation, testing, deployment, supply chain).*
- *CGRC: Governance, Risk & Compliance (7 domén: risk management, controls selection/implementation/assessment, authorization, monitoring).*
- *CCSK: Cloud security basics (12 oblastí: concepts, governance, risk/compliance, IAM, infrastructure/application/data security, incident response, encryption, virtualization).*

- *CompTIA Security+*: General security (5 domén: threats/vulnerabilities, architecture/design, implementation, operations/incident response, GRC).
- *UML2*: UML modelovanie (diagramy: class, sequence, state machine, object, package atď.). Zameraný na modelovanie systémov, nie security.

Podrobné porovnanie (pre prehľadnosť v tabuľke):

CCSP (Váha)	Doména	Pokrytie Kumuláciou	Hlavné Gaps (Medzery)	Celkové Hodnotenie Pokrytia
1. Cloud Concepts, Architecture and Design (17%)	(Cloud modely, architektúra, design princípy, virtualization, multi-tenancy, reference architectures ako NIST/ISO.)	Vysoké: CCSK (cloud concepts, architecture); CompTIA Security+ (architecture/design); UML2 (modelovanie architektúry cez diagramy); CSSLP (secure design).	Nedostatok špecifického fokusu na cloud reference models (napr. CSA CCM, NIST cloud framework). Chýba hĺbka v cloud-specific design risks (e.g., shared responsibility model). UML2 pomáha s modelovaním, ale nie s security aspektmi cloudu.	Stredný: Základy pokryté, ale chýba cloud-špecifická hĺbka. Odporúčam doplniť štúdium cloud architektúry.
2. Cloud Data Security (20%)	(Data lifecycle, encryption, tokenization, data loss prevention, database security, data classification v cloude.)	Stredné až vysoké: CCSK (data security, encryption); CompTIA Security+ (implementation security controls); CSSLP (secure implementation pre data); CISA (protection of information assets). CGRC (controls implementation).	Chýba špecifické cloud data handling (e.g., AWS S3 security, Azure data encryption at rest/transit). UML2 neprispievajú veľa. Nedostatok na data sovereignty a cloud-specific compliance (e.g., GDPR in multi-cloud).	Stredný: Dobré základy encryption a controls, ale gaps v cloud-specific tools a scenarios.
3. Cloud Platform & Infrastructure Security (17%)	(IaaS/PaaS security, network security, host security,	Vysoké: CCSK (infrastructure security, virtualization); CompTIA Security+ (architecture, implementation); CISA (operations/resilience);	Menej hĺbky v cloud platform-specific (e.g., AWS VPC, Azure NSG, container security ako Kubernetes).	Vysoký: Silné pokrytie infra security, minimálne gaps.

CCSP Doména (Váha)	Pokrytie Kumuláciou	Hlavné Gaps (Medzery)	Celkové Hodnotenie Pokrytia
virtualization security, BCP/DR v cloude.)	CGRC (continuous monitoring).	UML2 môže modelovať infra, ale nie secure ju. Chýba fokus na hypervisor attacks alebo cloud-native threats.	
4. Cloud Application Security (17%) (Secure SDLC v cloude, API security, serverless security, DevSecOps, application vulnerabilities.)	Vysoké: CSSLP (celý secure SDLC); CCSK (application security); CompTIA Security+ (vulnerabilities, implementation); CISA (acquisition/development). UML2 (modelovanie app design).	Chýba cloud-specific security (e.g., microservices, serverless ako Lambda, CI/CD in cloud).	Vysoký: CSSLP pokrýva veľa, gaps len v cloud-native apps.
5. Cloud Security Operations (19%) (Incident response, logging/monitoring, configuration management, vulnerability management, forensics v cloude.)	Vysoké: CompTIA Security+ (operations/incident response); CISA (operations); CGRC (monitoring); CCSK (incident response).	Nedostatok cloud-specific operations (e.g., AWS CloudTrail, Azure Sentinel, multi-cloud monitoring). Chýba hĺbka v automated ops (e.g., IaC security). UML2 neprispieva.	Vysoký: Dobré operačné znalosti, gaps v cloud tools.
6. Legal, Risk and Compliance (10%) (Legal requirements, risk management, compliance frameworks, audit v cloude, privacy.)	Vysoké: CGRC (GRC celé); CISA (governance, auditing); CCSK (risk, audit, compliance); CompTIA Security+ (GRC).	Chýba špecifické cloud compliance (e.g., FedRAMP, CSA STAR, cloud-specific risk assessments). UML2 a CSSLP neprispievajú.	Vysoký: Silné GRC základy, minimálne gaps.

Podrobná Textová Analýza

1. Cloud Concepts, Architecture and Design:

- Kumulácia poskytuje solidne základy cez CCSK (základné cloud concepts) a CompTIA Security+ (general architecture). UML2 pomáha s modelovaním (napr. class/use case diagrams pre design), CSSLP pridáva secure design princípy.
- Gaps: CCSP vyžaduje hĺbkové znalosti cloud models (IaaS/SaaS/PaaS), shared responsibility, a standards ako CSA CCM v4 alebo NIST SP 800-145. Kumulácia je všeobecnejšia (napr. bez cloud multi-tenancy risks). Kumulácia nezahŕňa cloud architecture training –
- Hodnotenie medzier (gaps): Vzhľadom na to, že IS RPO je prevádzkované v

privátnej časti vládneho cloudu a nie vo verejných cloudoch ani vo verejnej časti vládneho cloudu, je možné jednoznačne konštatovať že využité princípy IaaS Cloudu zodpovedajú štandardnej virtualizácii a v rámci RPO sú využívané štandardné virtualizované node servre. Preto je zrejme že tieto princípy v rámci riešenie IS RPO nie je možné uplatňovať.

2. Cloud Data Security:

- *Silné z CCSK (data security) a CompTIA (controls ako encryption). CSSLP pridáva secure implementation pre data handling, CISA chráni assets.*
- *Gaps: Špecifické cloud scenáre ako data in transit/rest v AWS/GCP, tokenization v multi-cloud, alebo data residency laws. UML2 sú irelevantné. Gap v praktických cloud tools (e.g., KMS services).*
- *Hodnotenie medzier (gaps): Vzhľadom na to, že cloud je prevádzkovaný a poskytovaný ako štandardná virtualizovaná infraštruktúra, nie je využívaný v rámci IS RPO žiadne KMS services. Takisto cloud je prevádzkovaný v zmysle zákona o IT VS preto ani otázky o multi-cloud riešení a data residency nie sú predmetom projektu IS RPO, nakoľko tieto požiadavky sú dané ako externé vstupy, a nie sú rozhodnutím projektu ISRPO.*

3. Cloud Platform & Infrastructure Security:

- *Vysoké pokrytie cez CCSK (infra/virtualization), CompTIA (design/implementation), CISA (resilience).*
- *Gaps: Menej na cloud-specific threats (e.g., side-channel attacks v virtualization, container orchestration security). CGRC pridáva monitoring, ale nie je infra-focused.*
- *Hodnotenie medzier (gaps): Za prevádzku infraštruktúry vládneho cloudu je zodpovedný poskytovateľ Ministerstvo vnútra SR. Cloud je poskytovaný z privátnej časti vládneho cloudu.*

4. Cloud Application Security:

- *Dominuje CSSLP (secure SDLC), doplnené CCSK (app security) a CompTIA (vulnerabilities). UML2 môže modelovať app flows.*
- *Gaps: Cloud-native apps (e.g., serverless, microservices security, API gateways v cloude). CISA pridáva development, ale nie cloud-specific.*
- *Hodnotenie medzier (gaps): IS RPO nie je vyvíjaná ako cloud natívna aplikácie, nakoľko vládny cloud neposkytuje služby, ktoré by umožnili vývoj cloud natívnych aplikácií. IS RPO je štandardná trojvrstvová aplikácia využívajúca IaaS služby privátneho vládneho cloudu a ani požiadavky nepopisujú požiadavku zmenu, resp. vývoj novej aplikácie, ktorá by zodpovedala cloud native aplikácii.*

5. Cloud Security Operations:

- *RESILIA a CompTIA excelujú v incident response/operations, CGRC v monitoring, CCSK v response.*
- *Gaps: Cloud forensics (e.g., log aggregation v Splunk for cloud), automated vulnerability scanning v cloude (e.g., AWS Inspector). Menej na ops v hybrid/multi-cloud.*

- *Hodnotenie medzier (gaps): IS RPO je umiestnené v cloud-e a nevyužíva natívne cloudové služby pre monitoring. Predmetom projektu RPO je len aplikačný monitoring aplikácie IS RPO. Služby agregácie logov, automatický vulnerability scanning a podobne sú z pohľadu projektu IS RPO externé služby a nie sú predmetom zákazky. ŠUSR disponuje SIEM (IBM QRadar,) ktorý realizuje tieto služby na všetkých IS ŠUSR. Avšak tieto služby sú mimo scope projektu RPO.*

6. Legal, Risk and Compliance:

- *CGRC a CISA pokrývajú GRC/auditing, CCSK pridáva compliance, CompTIA GRC.*
- *Gaps: Cloud-specific regs (e.g., PCI DSS in cloud, international data transfers). RESILIA pridáva risk, ale nie legal.*
- *Hodnotenie medzier (gaps): Legislatívne požiadavky na IS RPO a riziká sú riadené v zmysle platnej legislatívy, a to zákon o ITVS, Zákon o kybernetickej bezpečnosti a zákon o kritickej infraštruktúre. Zároveň v súlade s týmito požiadavkami je IS RPO umiestnený v privátnej časti vládneho cloudu, preto nie je možné naň primerane a adekvátne aplikovať požiadavky pri využívaní vládnych cloudov. PCI DSS a iné požiadavky na analýzu rizík a naplnenie legislatívnych požiadaviek zodpovedajú, napr. pre poskytovateľov platobných služieb (Payment Card Industry Data Security Standard). Preto tieto štandardy nie je možné aplikovať na IS RPO.*

Celkové Zhrnutie

- *Celkové pokrytie prostredníctvom kumulácie je stredne vysoké (cca 80 %). Kumulácia poskytuje silné základy v general security, GRC, auditing, software dev a cloud basics (vďaka CCSK), ale gaps sú hlavne v cloud-špecifických aspektoch (architecture, data/ops v cloud-e, native tools). UML2 pridáva modelovanie, čo je užitočné pre design, ale nie core pre security.*
- *Hlavné Gaps: Špecifická cloudu - kumulácia je široká, ale nie hlboká v cloud environments (e.g., AWS/Azure/GCP best practices, shared models).*

Dovoľujeme si uviesť, že pri posudzovaní ekvivalentnosti predložených certifikácií nie je možné ignorovať princíp prednosti materiálnej/obsahovej stránky veci a tým posudzovať ekvivalentnosť iba formálne. Je nutné vziať na zreteľ fakt, že smerom k verejnému obstarávateľovi nie je účelom podmienok účasti získať od uchádzača konkrétny dôkaz. Účelom je získať akýkoľvek relevantný dôkaz preukazujúci požadovanú mieru technickej a odbornej spôsobilosti uchádzača. V tomto konkrétnom prípade je tak účelom získať relevantné informácie o vzdelaní, znalostiach, praxi a praktických skúsenostiach kľúčového experta pre kybernetickú bezpečnosť na úrovni zodpovedajúcej povahe a zložitosti predmetu zákazky.

Máme za to, že sme dostatočne preukázali, že pán XXX disponuje vzdelaním, znalosťami, praxou a praktickými skúsenosťami pre oblasť kybernetickej bezpečnosti plne zodpovedajúcim úrovni zodpovedajúcej povahe a zložitosti predmetu zákazky. Vyššie popísané medzery totiž nemajú negatívny vplyv na kvalitu poskytovaných služieb nakoľko nie sú vo vzťahu k IS RPO a predmetu zákazky nutné. V súvislosti s pánom XXX sme tak podľa nášho názoru preukázali disponovanie ekvivalentnou technickou a odbornou spôsobilosťou. Požiadavku na ekvivalentnosť miery technickej spôsobilosti reprezentovanej požadovanou certifikáciou totiž vykladáme aj v zmysle všeobecne

akceptovaného právneho výkladu pojmu „ekvivalentnosť“ v oblasti verejného obstarávania kedy platí, že „...vyhodnocovanie ekvivalentnosti tovarov má zmysel práve pri tovaroch, ktoré síce všetky požiadavky na predmet zákazky nespĺňajú, avšak napriek tomu ich možno z určitého dôvodu považovať za rovnocenné. V prípade technického riešenia má ísť o také riešenie, ktoré plne zabezpečí plnenie predmetu zákazky definovaného verejným obstarávateľom“ (zdroj: Rozhodnutie Rady úradu č. 503-9000/2014-KR/5).

Máme za to, že takáto analogická aplikácia výkladu pojmu „ekvivalentný“ je v tomto prípade nielen formálne ale aj vecne prípustná a akceptovateľná, keďže sme preukázali, že pán XXX disponuje technickou a odbornou spôsobilosťou plne postačujúcou pre účely plnenia predmetu zákazky.

Odhladnuc od formálnej stránky veci je potrebné uviesť, že pán XXX disponuje aj samotným certifikátom CCSP, čím jednoznačne preukázal, že znalosťami, skúsenosťami a praxou potrebnými pre CCSP reálne disponoval, disponuje a disponovať bude. Máme za to, že ekvivalentnosť a dostatočnosť technickej a odbornej spôsobilosti vyplýva aj z jasne preukázanej dĺžky praxe v oblasti kybernetickej bezpečnosti ako aj rozsiahlych praktických skúseností s implementáciou projektov v oblasti kybernetickej bezpečnosti.

V prílohe prikladáme všetky požadované relevantné dokumenty. V prípade akýchkoľvek otázok nás neváhajte kontaktovať.“

Predmetná odpoveď navrhovateľa zároveň obsahovala nasledovné prílohy:

- životopis XXX (Špecialista IT bezpečnosti, Senior IT konzultant, audítor kybernetickej bezpečnosti)
- Certifikát Cloud Security Alliance udelený XXX za úspešné ukončenie a získanie Certificate of Cloud Security Knowledge v5 zo dňa 22. 01. 2025
- Certifikát GRC Professional (GRCP) udelený XXX za získanie kvalifikácie ako odborník v oblasti riadenia, manažmentu rizika a zhody (Governance, Risk Management and Compliance Professional – GRCP) zo dňa 26. 01. 2025
- Certifikát CISA – Certifikovaný audítor informačných systémov udelený XXX s dobou platnosti 08. 01. 2018 – 31. 01. 2025
- Certifikát CopmTIA, Security+, Certified CE udelený XXX s dobou platnosti 17. 10. 2024 – 17. 10. 2027
- Certifikát CSSLP pre bezpečný životný cyklus softvérov udelený XXX s dobou platnosti 01. 04. 2025 – 31. 05. 2028
- Certifikát CISA – Certifikovaný audítor informačných systémov udelený XXX s dobou platnosti 08. 01. 2018 – 31. 01. 2028
- Certifikát OMG - Certified UML Professional 2 (OCUP 2) – Pokročilá úroveň zo dňa 18. 11. 2021 s platnosťou 5 rokov od dátumu vystavenia
- Znalecký posudok č. 13/2025 vypracovaný znaleckou organizáciou Kompetenčné a certifikačné centrum kybernetickej bezpečnosti vo veci zodpovedania otázok k ekvivalentnosti certifikátov.

72. Kontrolovaný následne dňa 26. 11. 2025 doručil navrhovateľovi Oznámenie o výsledku vyhodnotenia ponúk, v ktorom uviedol, že cit.: „na základe kritéria na vyhodnotenie ponúk sa

na prvom mieste umiestnila ponuka spoločnosti XX, ktorá zároveň preukázala splnenie všetkých podmienok účasti a požiadaviek na predmet zákazky. Ponuka úspešného uchádzača je pre verejného obstarávateľa výhodná, keďže v plnej miere splňa ním stanovené požiadavky na predmet obstarávania tak po stránke technickej, ako aj ekonomickej.“ Kontrolovaný zároveň doručil navrhovateľovi Prílohu č. 1 Oznámenia o výsledku vyhodnotenia ponúk, ktorú dňa 01. 12. 2025 z dôvodu chýb v pôvodnej prílohe zo dňa 26. 11. 2025 aktualizoval.

73. Úrad uvádza, že Príloha č. 1 Oznámenia o výsledku vyhodnotenia ponúk zo dňa 01. 12. 2025 obsahuje oproti Prílohe č. 1 zo dňa 20. 08. 2025 (ktorá bola preskúmaná v rámci konania úradu č. 11915-6000/2025) jedinú odlišnosť spočívajúcu v dodatočnej strane predmetnej prílohy spočívajúcej v zachytení procesu opätovného vyhodnotenia podmienok účasti u úspešného uchádzača, a to v rozsahu, cit.:

„Požiadavka podľa SP	Predložené v ponuke / pôvodne	Doplnené / predložené neskôr (v procese)	Poznámka pre znovuvyhodnotenie
CCSP (Certified Cloud Security Professional) alebo ekvivalent	Certificate of Cloud Security Knowledge v5 (uvedené ako „namiesto CCSP“)	CCSP (Certified Cloud Security Professional) – vydaný pre XXX (komisia overovala platnosť cez ISC2 Member Verification; uvádzaný dátum začatia platnosti 14.07.2025)	požiadavka naplnená predložením CCSP certifikátu Na základe predloženého dokladu a jeho obsahového posúdenia (vrátane znaleckého posudku) komisia konštatuje splnenie požiadavky.
CSSLP (Certified Secure Software Lifecycle Professional) alebo ekvivalent	CompTIA Security+ Certified CE (uvedené ako „namiesto CSSLP“)	CSSLP – vydaný pre XXX (komisia overovala platnosť cez ISC2 Member Verification; uvádzaný dátum začatia platnosti 03.03.2025)	požiadavka naplnená predložením CSSLP certifikátu. Na základe predloženého dokladu a jeho obsahového posúdenia (vrátane znaleckého posudku) komisia konštatuje splnenie požiadavky.
CGRC (Certified Governance, Risk and Compliance) alebo ekvivalent	Predložený certifikát ako ekvivalent: Certified GRC Professional (GRCP)	(v rozhodnutí sa rieši najmä námietka k ekvivalentnosti GRCP ↔ CGRC; ÚVO uvádza, že sa ekvivalentnosťou v tej časti už nezaoberal z dôvodu procesnej situácie)	požiadavka naplnená predložením GRCP + znalecký posudok Na základe predloženého dokladu a jeho obsahového posúdenia (vrátane znaleckého posudku) komisia konštatuje splnenie požiadavky.“

74. Úrad posúdi proces vyhodnocovania splnenia podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému odborníkovi č. 6 „Špecialista na

bezpečnosť“ u úspešného uchádzača, ktorý bol zároveň predmetom právneho posúdenia úradu v predchádzajúcom rozhodnutí úradu, a teda **či kontrolovaný vyhodnotil podmienky účasti u úspešného uchádzača odstrániac úradom identifikované pochybenia rozporné so zákonom o verejnom obstarávaní.**

75. Úrad konštatuje, že v časti 2. „Technická spôsobilosť alebo odborná spôsobilosť“, v bode 2.5 súťažných podkladov sú uvedené nasledovné požiadavky na kľúčového odborníka – Špecialistu na bezpečnosť, ktorých splnenie úspešný uchádzač preukazoval XXX, cit.:

(...)

2.5.6 kľúčový odborník - Špecialista na bezpečnosť (min. 1 osoba), ktorý musí spĺňať nasledovné minimálne požiadavky odbornej praxe a odbornej kvalifikácie:

(...)

- *platný certifikát pre CCSP (Certified Cloud Security Professional), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);*
- *platný certifikát pre CSSLP (Certified Secure Software Lifecycle Professional, alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač);*
- *platný certifikát pre CGRC (Certified Governance, Risk and Compliance), alebo ekvivalent daného certifikátu vydaný medzinárodne uznávanou akreditovanou (certifikovanou) autoritou; túto požiadavku uchádzač preukáže predložením požadovaného certifikátu, alebo ekvivalentu daného certifikátu (ekvivalentnosť predloženého certifikátu preukazuje uchádzač).“*

76. Úrad uvádza, že v predchádzajúcom rozhodnutí posudzoval:

- a) v časti Ad 1. „certifikát CCSP (Certified Cloud Security Professional)“ platnosť predmetného certifikátu vo vzťahu k lehote na predkladanie ponúk, a teda jeho aprobáciu kontrolovaným ako dokladu preukazujúceho splnenie podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní;
- b) v časti Ad 2. „certifikát CGRC (Certified Governance, Risk and Compliance)“ ekvivalentnosť úspešným uchádzačom predloženého certifikátu Certified GRC Professional (GRCP) ku kontrolovanému certifikátu CGRC (Certified Governance, Risk and Compliance);

pričom v námietkach navrhovateľa, ktoré sú predmetom tohto konania navrhovateľ spochybňuje aj certifikát CSSLP (Certified Secure Software Lifecycle Professional), a to vo vzťahu k fáze, v ktorej bol úspešným uchádzačom predložený (t. j. po lehote na predkladanie ponúk v rámci odpovede na žiadosť o nahradenie osôb určených na plnenie zmluvy) ako aj samotné vyhodnocovanie predmetného certifikátu kontrolovaným v rozpore s predchádzajúcim rozhodnutím úradu.

77. Úrad sa v predchádzajúcom rozhodnutí zaoberal spôsobom, akým sa kontrolovaný vysporiadal s predložením nových dokladov za XXX – kľúčového odborníka – Špecialistu na bezpečnosť, keď namiesto nahradenia tejto osoby v nadväznosti na žiadosť o nahradenie osôb určených na

plnenie zmluvy úspešný uchádzač dodatočne predložil doklady na preukázanie splnenia podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní (aj) vo vzťahu ku kľúčovému odborníkovi č. 6 – Špecialista na bezpečnosť, XXX. Úrad v bodoch 81 a 82 predmetného rozhodnutia skonštatoval, cit.: „81. (...) úspešný uchádzač kľúčového odborníka Špecialista na bezpečnosť - XXX, v reakcii na žiadosť kontrolovaného, nenahradil ani jedným zo zákonom aprobovaných spôsobov, t. j. **nereagoval na žiadosť o nahradenie osôb určených na plnenie zmluvy v súlade s požiadavkou kontrolovaného, ale predložil nové doklady za toho istého kľúčového odborníka Špecialistu na bezpečnosť – XXX, čo však kontrolovaný pri vyhodnocovaní splnenia podmienok účasti nezohľadnil.**

82. Úrad konštatuje, že kontrolovaný postupoval pri vyhodnocovaní podmienok účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní u úspešného uchádzača v rozpore so zákonom o verejnom obstarávaní, keď úspešný uchádzač po žiadosti o nahradenie osôb určených na plnenie zmluvy, XXX v pozícii kľúčového experta – Špecialista na bezpečnosť, z dôvodu nesplnenia podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní, predmetného odborníka nenahradil, a kontrolovaný napriek tomu túto skutočnosť akceptoval. Inými slovami, kontrolovaný akceptoval dodatočne predložené doklady (certifikáty) k predmetnému expertovi, ktoré mu boli úspešným uchádzačom doručené v reakcii na žiadosť o nahradenie, pričom kontrolovaný ďalej netrval na nahradení tohto experta. Úrad konštatuje, že kontrolovaný nemôže po tom, čo uchádzača požiada o nahradenie konkrétneho kľúčového odborníka takpovediac negovať predmetnú žiadosť a následky z nej vyplývajúce tým, že prijme ponuku uchádzača, u ktorého už raz identifikoval nesplnenie podmienok účasti a u ktorého s ohľadom na skutočnosť, že k nahradeniu Špecialistu na bezpečnosť XXX nedošlo, nesplnenie podmienok účasti stále trvá.“ Kontrolovaný napriek úradom deklarovanému nezákonnému postupu zvolil aj po právoplatnosti prechádzajúceho rozhodnutia úradu postup opätovného skúmania splnenia podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému odborníkovi č. 6 – Špecialista na bezpečnosť, XXX u úspešného uchádzača, a to prostredníctvom žiadosti o vysvetlenie.

78. Úrad v tejto súvislosti konštatuje, že žiadosť o vysvetlenie nasledujúca po právoplatnosti predchádzajúceho rozhodnutia úradu a odpoveď úspešného uchádzača, ktorá bola ďalej zo strany kontrolovaného podrobovaná vyhodnocovaniu stráca opodstatnenie, a to s ohľadom na pochybenia kontrolovaného v procese vyhodnocovania splnenia podmienok účasti u úspešného uchádzača – konkrétne **s ohľadom na fázu vyhodnocovania**, v ktorej sa kontrolovaný pochybenia dopustil. Nemožno teda stavať legitímnosť vyhodnotenia splnenia podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní na nezákonnom základe spočívajúcom v neaplikovaní § 40 ods. 6 písm. j) zákona o verejnom obstarávaní, pokiaľ ním predpokladaná situácia preukázateľne nastala, a teda aprobovať vyhodnocovanie úspešným uchádzačom predložených dokumentov/certifikátov (či už v rámci odpovede na žiadosť o nahradenie osôb určených na plnenie zmluvy alebo v rámci odpovede na žiadosť o vysvetlenie), pokiaľ k takémuto predkladaniu dokumentov (t. j. vo fáze po žiadosti podľa § 40 ods. 5 písm. c) zákona o verejnom obstarávaní) vôbec nemalo dôjsť. A to aj za situácie, keby úspešný uchádzač dodatočne predloženými certifikátmi za XXX bol schopný splnenie predmetnej podmienky účasti preukázať, nakoľko pokiaľ úspešný uchádzač disponoval certifikátmi relevantnými pre splnenie podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní vo vzťahu ku kľúčovému odborníkovi – Špecialista na bezpečnosť, tieto mali byť súčasťou jeho ponuky, resp. s ohľadom na využitie inštitútu JED-u

podľa § 39 zákona o verejnom obstarávaní, súčasťou predložených dokladov, ktoré JED-om nahrádzal.

79. Metodické usmernenie úradu č. [16186-5000/2023](#) zo dňa 28. 11. 2023 poukazuje na zodpovednosť uchádzača za doklady predkladané vo svojej ponuke, a to cit.: „**Zostavenie a predloženie ponuky je vecou uchádzača, ktorý zodpovedá za jej obsah. Uchádzač by mal pritom plne reflektovať požiadavky verejného obstarávateľa uvedené v dokumentoch potrebných na vypracovanie ponuky. Ponuka by mala obsahovať všetky relevantné informácie a jej obsah by mal byť dostatočne zrozumiteľný na to, aby ju verejný obstarávateľ mohol riadne vyhodnotiť podľa ním stanovených kritérií.**“
80. Úrad konštatuje, že kontrolovaný z dokladov z ponuky úspešného uchádzača, resp. z dokladov nahradených JED-om deklaroval nesplnenie podmienok účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní a následne úspešnému uchádzačovi dňa 25. 07. 2025 doručil v súlade s § 40 ods. 5 písm. c)² zákona o verejnom obstarávaní žiadosť o nahradenie osôb určených na plnenie zmluvy, ktorá zahŕňala aj nahradenie XXX na pozícii kľúčového experta č. 6 – Špecialista na bezpečnosť, pričom úspešný uchádzač XXX v pozícii predmetného kľúčového experta nenahradil. Úrad poukazuje na metodické usmernenie úradu č. [9806-5000/2021](#) zo dňa 09. 08. 2022, ktoré pojednáva o význame nahradenia osôb nespĺňajúcich stanovené podmienky účasti, cit.: „**Pod nahradením v kontexte vyššie uvedených ustanovení zákona o verejnom obstarávaní je potrebné rozumieť zámenu osoby, ktorá nespĺňa stanovené podmienky účasti, resp. existuje u nej dôvod na vylúčenie. Výzva verejného obstarávateľa/obstarávateľa na nahradenie automaticky nespôsobí vylúčenie uchádzača alebo záujemcu, ale ponúka mu možnosť prostredníctvom inštitútu nahradenia preukázať splnenie podmienok účasti týkajúcich sa finančného a ekonomického postavenia a technickej a odbornej spôsobilosti novým subjektom, ktorý bude spĺňať podmienky účasti, resp. u neho nebude existovať dôvod na vylúčenie. Zákonodarcu dáva týmto inštitútom teda uchádzačovi alebo záujemcovi možnosť zotrvať vo verejnom obstarávaní, v prípade, ak vie prostredníctvom nového subjektu preukázať finančné a ekonomické postavenie, resp. odbornú a technickú spôsobilosť.**“ Úspešný uchádzač však v odpovedi na žiadosť o nahradenie osôb určených na plnenie zmluvy k zámene kľúčového experta č. 6 v podobe XXX za inú osobu spĺňajúcu predmetnú podmienku účasti **nepristúpil**.
81. Úrad v tejto súvislosti poukazuje na ustanovenie § 40 ods. 6 písm. j) zákona o verejnom obstarávaní konštituujuce **obligatórnu povinnosť verejného obstarávateľa alebo obstarávateľa pristúpiť k vylúčeniu uchádzača, ktorý si povinnosť nahradenia inej osoby** (prostredníctvom ktorej úspešný uchádzač preukazuje splnenie podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní) **nesplnil, k čomu však kontrolovaný nepristúpil**. Uvedený prístup potvrdzuje aj rozhodnutie predsedu úradu č. [15174-9000/2024](#) zo dňa 26. 11. 2024 v bode 75, kde predseda úradu skonštatoval, cit.: „**Predseda úradu uvádza, že podľa § 40 ods. 5 písm. c) zákona o verejnom obstarávaní verejný obstarávateľ a obstarávateľ sú povinní písomne požiadať uchádzača alebo záujemcu, aby v lehote, ktorá nesmie byť kratšia ako päť pracovných dní odo dňa doručenia žiadosti, nahradil inú osobu, ktorej prostredníctvom preukazuje finančné a ekonomické postavenie alebo technickú spôsobilosť alebo odbornú**

² Žiadosť o nahradenie osôb určených na plnenie zmluvy kontrolovaný koncipoval podľa § 40 ods. 5 písm. b) zákona o verejnom obstarávaní, pričom túto skutočnosť úrad ozrejmil v bodoch 69. – 71. predchádzajúceho rozhodnutia úradu.

spôsobilosť, ak existujú dôvody na jej vylúčenie. Z citovaného zákonného ustanovenia vyplýva, že verejný obstarávateľ je **povinný písomne požiadať uchádzača o nahradenie inej osoby, prostredníctvom ktorej preukazuje finančné a ekonomické postavenie alebo technickú spôsobilosť alebo odbornú spôsobilosť, ak existujú dôvody na vylúčenie tejto inej osoby.** V prvom rade predseda úradu uvádza, že zákon o verejnom obstarávaní explicitne podmieňuje nahradenie inej osoby skutočnosťou, že u inej osoby existujú dôvody na jej vylúčenie, pričom v tejto súvislosti zákon o verejnom obstarávaní nekonkretizuje, aké dôvody vylúčenia je možné aplikovať vo vzťahu k inej osobe, či už explicitnou úpravou alebo odkazom na vylučovacie dôvody vzťahujúce sa na záujemcu/uchádzača, resp. na vylúčenie ponuky. Teda zákon o verejnom obstarávaní nezužuje aplikáciu inštitútu nahradenia inej osoby len na situáciu, ak iná osoba nespĺňa podmienky účasti (ako uvádza úrad v bode 136 rozhodnutia), ale umožňuje inštitút nahradenia inej osoby aplikovať v rámci širšieho diapazónu dôvodov na vylúčenie, ktoré upravuje zákon o verejnom obstarávaní vo vzťahu k uchádzačom/ záujemcom a ktoré sú funkčne aplikovateľné aj na iné osoby. (...)“.

82. Dôsledok takéhoto konania úspešného uchádzača je predvídaný ustanovením § 40 ods. 6 písm.

j) zákona o verejnom obstarávaní, podľa ktorého, cit.: „**Verejný obstarávateľ a obstarávateľ vylúčia kedykoľvek počas verejného obstarávania uchádzača alebo záujemcu, ak nenahradil inú osobu, prostredníctvom ktorej preukazuje splnenie podmienok účasti finančného a ekonomického postavenia alebo technickej spôsobilosti alebo odbornej spôsobilosti, ktorá nespĺňa určené požiadavky, v určenej lehote inou osobou, ktorá spĺňa určené požiadavky.**“ Vo vzťahu ku kogentnosti uvedeného ustanovenia zákona úrad poukazuje na rozhodnutie Rady úradu č. [7614-9000/2019](#) zo dňa 01. 07. 2019, cit.: „156. Rada má za to, že ustanovenie § 40 ods. 6 zákona o verejnom obstarávaní (...), ktoré upravuje dôvody vylúčenia uchádzačov, je koncipované ako kogentné, t. j. **ukladajúce verejnému obstarávateľovi povinnosť vylúčiť uchádzača, ak dôjde k naplneniu niektorého z uvedených dôvodov.** Verejní obstarávatelia teda v prípade zistenia dôvodu upraveného v § 40 ods. 6 zákona o verejnom obstarávaní **nemajú na výber, či pristúpia k jeho vylúčeniu z procesu verejného obstarávania alebo ho napriek tomu ponechajú v súťazi.**

157. Samozrejme, v súlade s princípom rovnakého zaobchádzania s uchádzačmi a záujemcami podľa § 10 ods. 2 zákona o verejnom obstarávaní, ktorý sa musí uplatňovať vo vzťahu ku všetkým uchádzačom v priebehu celého procesu verejného obstarávania, musí verejný obstarávateľ pri aplikácii § 40 ods. 6 tohto zákona postupovať rovnako pri všetkých uchádzačoch. Z toho tiež vyplýva, že **žiadneho z uchádzačov nemôže zvýhodniť tým, že by v jeho prípade nepristúpil k vylúčeniu z verejného obstarávania, ak nastal dôvod na jeho vylúčenie a súčasne žiadneho z uchádzačov nemôže znevýhodniť (napr. tým, že by podmienky účasti v jeho prípade posudzoval inak – prísnejšie ako u iných uchádzačov v rovnakom postavení).**“

83. Na základe vyššie uvedených skutočností úrad konštatuje, že kontrolovaný po doručení odpovede úspešného uchádzača na žiadosť o nahradenie osôb určených na plnenie zmluvy nesúladnej s ustanovením § 40 ods. 5 písm. c) zákona o verejnom obstarávaní a samotným znením predmetnej žiadosti, t. j. úspešný uchádzač XXX na pozícii kľúčového experta č. 6 – Špecialista na bezpečnosť, nepristúpil vo vzťahu k vyhodnoteniu predmetnej podmienky účasti u úspešného uchádzača k postupu, ktorý kontrolovanému z ustanovenia § 40 ods. 6 písm. j) zákona o verejnom obstarávaní vyplýva. Kontrolovaný sa tak dopustil porušenia predmetných ustanovení zákona o verejnom obstarávaní, ako aj princípov transparentnosti a rovnakého zaobchádzania, nakoľko predmetným

konaním zvýhodnil úspešného uchádzača aj napriek v žiadosti o nahradenie osôb určených na plnenie zmluvy deklarovanému nesplneniu podmienok účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní. Úrad na margo uvedeného dodáva, že predmetným konaním kontrolovaného nedošlo k odstráneniu pochybení identifikovaných v rozhodnutí úradu č. 11915-6000/2025 zo dňa 29. 09. 2025, čím vzniknutý nezákonný stav naďalej trvá.

84. V kontexte vyššie uvedených skutočností úrad považuje námietky navrhovateľa za **opodstatnené**.

85. V zmysle ustanovenia § 175 ods. 8 písm. a) zákona o verejnom obstarávaní úrad konštatuje, že kontrolovaný nezohľadniac povinnosť vyplývajúcu mu z ustanovenia § 40 ods. 6 písm. j) zákona o verejnom obstarávaní pristúpil k vyhodnocovaniu dokladov/certifikátov predložených úspešným uchádzačom v rámci odpovede na žiadosť o nahradenie osôb určených na plnenie zmluvy a v rámci odpovede na žiadosť o vysvetlenie, čo zároveň koliduje s princípmi verejného obstarávania zakotvenými v ustanovení § 10 ods. 2 zákona o verejnom obstarávaní, a to najmä s princípom transparentnosti a princípom rovnakého zaobchádzania, teda k postupu nesúladnému so zákonom o verejnom obstarávaní. Identifikované porušenia zákona o verejnom obstarávaní v tomto prípade mohli mať vplyv na výsledok verejného obstarávania, keďže objektívna stránka identifikovaného porušenia zákona o verejnom obstarávaní spočíva vo vyhodnotení spoločnosti XX ako úspešného uchádzača napriek skutočnosti, že úspešný uchádzač v odpovedi na žiadosť o nahradenie osôb určených na plnenie zmluvy uplatnenú kontrolovaným v súlade s § 40 ods. 5 písm. c) zákona o verejnom obstarávaní, XXX v pozícii kľúčového odborníka č. 6 – Špecialista na bezpečnosť, nenahradil, na základe čoho nemožno jednoznačne vysloviť záver, že by predmetné verejné obstarávanie smerovalo k výberu takého zmluvného partnera, ktorý by vzišiel zo zákazky zadávanej v súlade so zákonom o verejnom obstarávaní, resp. zo zákazky, ktorej priebeh nevykazuje znaky porušenia tohto zákona.

86. Úrad v zmysle ustanovenia § 175 ods. 8 písm. b) zákona o verejnom obstarávaní kontrolovanému odporúča za účelom predchádzania identifikovaným porušeniam zákona o verejnom obstarávaní *pro futuro*, aby **kontrolovaný pri vyhodnocovaní splnenia podmienok účasti dbal na dodržiavanie povinností viažucich sa k nenahradeniu osôb určených na plnenie zmluvy podľa § 40 ods. 6 písm. j) zákona o verejnom obstarávaní zohľadňujúc jeho účel naviazaný na nesplnenie podmienky účasti podľa § 34 ods. 1 písm. g) zákona o verejnom obstarávaní v prípade konkrétneho kľúčového odborníka.**

87. Na základe všetkých uvedených skutočností bolo vo vzťahu k námietkam navrhovateľa potrebné rozhodnúť tak, ako je uvedené vo výrokovej časti tohto rozhodnutia.

88. Podľa § 175 ods. 10 zákona o verejnom obstarávaní sa rozhodnutie podľa § 175 ods. 1 písm. a) až c) sa zároveň doručuje úradu známym uchádzačom a účastníkom.

Kaucia

Podľa 172 ods. 5 zákona o verejnom obstarávaní kaucia vo výške podľa odsekov 2 až 4 je príjmom štátneho rozpočtu dňom nadobudnutia právoplatnosti rozhodnutia úradu, ktorým boli námietky v celom rozsahu zamietnuté, alebo dňom nadobudnutia právoplatnosti rozhodnutia

úradu o zastavení konania podľa § 174 ods. 1 písm. p) zákona o verejnom obstarávaní. Kaucia sa vo výške 50 % z výšky kaucie podľa odsekov 2 až 4 stáva príjmom štátneho rozpočtu dňom nadobudnutia právoplatnosti rozhodnutia úradu o zastavení konania podľa § 174 ods. 1 písm. d) zákona o verejnom obstarávaní. Úrad vráti navrhovateľovi kauciu alebo jej časť, ktorá sa nestala príjmom štátneho rozpočtu, do 30 dní odo dňa právoplatnosti rozhodnutia.

89. V súlade s týmto ustanovením zákona o verejnom obstarávaní a výrokom tohto rozhodnutia úrad vráti navrhovateľovi kauciu zloženú za podanie námietok v plnej výške, a to do 30 dní odo dňa nadobudnutia právoplatnosti tohto rozhodnutia.

P o u č e n i e:

Podľa § 175 ods. 11 zákona o verejnom obstarávaní proti tomuto rozhodnutiu úradu nie je možné podať riadny opravný prostriedok. Podľa § 52 zákona č. 71/1967 Zb. o správnom konaní (správny poriadok) v znení neskorších predpisov v spojení s § 185 ods. 2 zákona o verejnom obstarávaní je toto rozhodnutie právoplatné dňom doručenia účastníkom konania a všetkým úradu známym uchádzačom a vykonateľné uplynutím lehoty na plnenie. Podľa § 175 ods. 11 druhá veta zákona o verejnom obstarávaní rozhodnutie v námietkovom konaní je preskúmateľné súdom, pričom žaloba musí byť podaná do 30 dní odo dňa doručenia rozhodnutia.

(elektronický podpis)

JUDr. Štefan Halický
generálny riaditeľ sekcie dohľadu

Rozhodnutie sa doručí:

1. **XY** – navrhovateľ
2. **Štatistický úrad Slovenskej republiky**, Lamačská cesta 3/C, 840 05 Bratislava – mestská časť Karlova Ves, IČO: 00 166 197 – kontrolovaný

Na vedomie:

3. Podľa rozdeľovníka