MINISTERSTVO
ŠKOLSTVA, VÝSKUMU,
VÝVOJA A MLÁDEŽE
SLOVENSKEJ REPUBLIKY

Zápisnica z vyhodnotenia splnenia podmienok účasti

podľa § 40 zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov

1. Názov verejného obstarávateľa/prijímateľa: Ministerstvo školstva, výskumu, vývoja a mládeže SR
2. Sídlo verejného obstarávateľa/prijímateľa: Černyševského 50, 851 01 Bratislava
3. Predmet/názov zákazky: Digitálna infraštruktúra škôl - vytvorenie riešenia na školách a prevádzka komplexných telekomunikačných služieb LAN/WLAN/WAN Košický kraj
4. Druh postupu: nadlimitná zákazka – verejná súťaž
5. Druh zákazky: zákazka na poskytnutie služieb podľa § 3 ods. 4 ZVO
6. Predpokladaná hodnota zákazky: 34 397 641,35 EUR bez DPH
7. Označenie v Úradnom vestníku EÚ: č. S253/2024 dňa 31.12.2024 pod číslom 800967-2024
8. Označenie vo Vestníku VO: č. 1/2025 dňa 02.01.2025 pod označením 12 – MSS
9. Dátum vyhodnotenia: od 14.02.2025 do 01.07.2025
10. Miesto vyhodnotenia: Černyševského 50, 851 01 Bratislava
11. Členovia komisie:
    Ing. Alexander Šproch – predseda komisie s právom vyhodnocovať ponuky a komunikovať v mene zadávateľa
    Ing. Ján Jasenák– člen komisie s právom vyhodnocovať ponuky
    Ing. Ivan Šiagi – člen komisie s právom vyhodnocovať ponuky
    Ing. Štefan Mačica - člen komisie s právom vyhodnocovať ponuky
    Ing. Vladimír Pokojný– člen komisie bez práva vyhodnocovať ponuky, administrátor zákazky
    Mgr. Silvia Schlosserová – členka komisie bez práva vyhodnocovať ponuky, administrátor zákazky
12. Predložené žiadosti o vysvetlenie podľa § 48 ZVO: zoznam otázok doručených v rámci žiadostí o vysvetlenie a odpovedí je zverejnený na profile verejného obstarávateľa v dokumentácii k danej zákazke
13. Zoznam uchádzačov/záujemcov:

Poradové číslo	Uchádzač/Skupina dodávateľov	Dátum a čas predloženia ponuky	Spôsob predloženia ponuky
1	**Slovanet, a.s.** Galvaniho 19 821 04 Bratislava IČO: 35954612	13.02.2025 01:28:08	42 848 595,06 EUR bez DPH
2	**Slovak Telekom, a.s.** Bajkalská 28 817 62 Bratislava IČO: 35763469	13.02.2025 13:23:09	42 419 181,40 EUR bez DPH

Poradové číslo	Uchádzač/Skupina dodávateľov	Dátum a čas predloženia ponuky	Spôsob predloženia ponuky
3	**SWAN, a.s.** Landererova 12 811 09 Bratislava IČO: 35680202	13.02.2025 13:44:39	39 587 047,32 EUR bez DPH
4	**O2 Business Services, a.s.** Pribinova 40 811 09 Bratislava IČO: 50087487	13.02.2025 20:37:41	42 785 921,76 EUR bez DPH
5	**ANTIK Telekom, s.r.o.** Čárskeho 10 04 001 Košice IČO: 36191400	14.02.2025 09:58:04	42 714 275,99 EUR bez DPH

14. Vyhodnotenie splnenia podmienok účasti:

Podľa Časti A.1 Súťažných podkladov – Pokyny pre uchádzačov, bodu 9.2: *„Verejný obstarávateľ uzavrie s viacerými, t. j. s úspešnými uchádzačmi na základe výsledku verejného obstarávania „Rámcovú dohodu s opätovným otváraním“ podľa § 83 ods. 5 písm. b) zákona o verejnom obstarávaní.“*

Pri vyhodnotení splnenia podmienok účasti komisia postupovala v súlade s § 40 ZVO a vyhodnocovala všetky predložené ponuky.

V súlade s § 39 ods. 6 ZVO požiadala komisia dňa 18.02.2025 uchádzačov č. 1 Slovanet, a.s., uchádzača č. 3 SWAN, a.s. a uchádzača č. 5 Antik Telekom, s.r.o. prostredníctvom systému IS Josephine o predloženie dokladov predbežne nahradených JEDom.

Lehota na predloženie dokladov preukazujúcich splnenie podmienok účasti predbežne nahradených JEDom bola stanovená do 27.02.2025 do 11:00 hod.

Uchádzač č. 1 Slovanet, a.s., uchádzač č. 3 SWAN, a.s. a uchádzač č. 5 Antik Telekom, s.r.o. predložili doklady preukazujúce splnenie podmienok účasti a súčasne v súlade s § 39 ZVO predložili Jednotný európsky dokument (JED), v ktorom označili globálny údaj preukazujúci splnenie podmienok účasti.

Uchádzač č. 3 SWAN, a. s. doručil odpoveď dňa 21.02.2025 o 18:40 hod.

Komisia konštatuje, že vysvetlenie bolo doručené v stanovenej lehote.

Vo svojej odpovedi uchádzač č. 3 SWAN, a.s. uviedol: *„Máme za to, že sme predložili verejnému obstarávateľovi v rámci ponuky všetky požadované doklady na preukázanie splnenia podmienok účasti. V rámci jednotného európskeho dokumentu sme verejnému obstarávateľovi uviedli požadované údaje o našej spoločnosti a tiež, že sme spoločnosť zapísaná v zozname hospodárskych subjektov pod č. 2024/11-PO-F7847. Na základe Vašej žiadosti Vám posielame v prílohe výpis zo ZHS zo stránky ÚVO uvo.gov.sk.*

V prípade, že identifikujete v nami v ponuke predložených dokladoch na preukázanie splnenia podmienok účasti nejaké konkrétne nedostatky, sme pripravení ich vysvetliť prípadne doplniť.“

Komisia konštatuje, že uchádzač č. 3 SWAN, a.s. predložil všetky požadované doklady.

Uchádzač č. 1 Slovanet, a. s. doručil odpoveď dňa 24.02.2025 o 21:11 hod.

Komisia konštatuje, že vysvetlenie bolo doručené v stanovenej lehote.

Vo svojej odpovedi uchádzač č. 1 Slovanet, a.s. uviedol: *„Uchádzač v rámci svojej ponuky predložil Krycí list ponuky, ktorý v jednej zo svojich častí okrem iného pozostáva z Obsahu ponuky, v rámci ktorého Uchádzač uviedol, ktoré dokumenty pre preukázanie podmienok účasti podľa § 32, § 34 a § 35 vo väzbe na § 34 ZoVO použil. Máme za to, že ak uchádzač v ponuke predloží súčasne Jednotný európsky dokument (JED) aj doklady preukazujúce splnenie podmienok účasti, verejný obstarávateľ má možnosť uprednostniť na zabezpečenie riadneho priebehu verejného obstarávania predložené doklady preukazujúce splnenie podmienok účasti pred Jednotným európskym dokumentom, čím sa zabezpečí efektívnejší a rýchlejší proces overovania splnenia podmienok účasti. Uchádzač v súčasnosti nedisponuje informáciou o tom, či posúdenie dokladov preukazujúcich splnenie podmienok účasti uvedených v ponuke uchádzača komisia vyhodnotila po obsahovej stránke ako obsahovo úplné alebo nie. Z daného dôvodu Uchádzač v prílohe tejto odpovede Verejnému obstarávateľovi opätovne doručuje doklady a dokumenty preukazujúce splnenie podmienok účasti podľa § 32, § 34 a § 35 vo väzbe na § 34 ZoVO v súlade s požiadavkou zo dňa 18.02.2025 vo väzbe na ust. § 39 ods. 6 ZoVO. Uchádzač si v tejto súvislosti dovoľuje uviesť, že využitie Jednotného európskeho dokumentu je fakultatívnym inštitútom, čo umožňuje jeho využitie v ponuke uchádzača súčasne aj s dokumentami preukazujúcimi splnenie podmienok účasti. V prípade, že by napriek poskytnutému vyjadreniu Verejný obstarávateľ identifikoval akékoľvek ďalšie nejasnosti/nezrovnalosti, je tieto Uchádzač pripravený náležite vysvetliť.“*

Prílohou odpovede boli všetky dokumenty preukazujúce splnenie podmienok účasti. Komisia kontrolou dokumentov predložených v ponuke a dokumentov predložených v rámci odpovede zistila, že obe sady dokumentov preukazujúcich splnenie podmienok účasti sú totožné.

Komisia konštatuje, že uchádzač č. 1 Slovanet, a.s. predložil všetky požadované doklady.

Uchádzač č. 5 Antik Telekom, s.r.o. doručil odpoveď dňa 27.02.2025 o 10:24 hod.

Komisia konštatuje, že vysvetlenie bolo doručené v stanovenej lehote.

Vo svojej odpovedi uchádzač č. 5 Antik Telekom, s.r.o. uviedol: *„V prílohách dopĺňame dokumenty“.*

Komisia konštatuje, že uchádzač č. 5 Antik Telekom, s.r.o. predložil všetky požadované doklady.

Kontrola zloženia zábezpeky:

Podľa súťažných podkladov časti A.1 Pokyny pre záujemcov a uchádzačov bodu 18 bola požadovaná zábezpeka vo výške 300 000,00 EUR

Uchádzač č. 1 Slovanet, a.s. vo svojej ponuke predložil Bankovú záruku č. 626.826 zo dňa 11.02.2025 vystavenú Tatra bankou, a.s.. Banková záruka je podpísaná elektronickou pečaťou TB.

Z predloženej záruky vyplýva, že Banka sa zaväzuje vykonať platbu Obstarávateľovi do vyššie uvedenej sumy po predložení jeho prvej písomnej výzvy na zaplatenie, za podmienky, že Obstarávateľ v písomnej výzve na zaplatenie uvedie, že suma, ktorú požaduje, je splatná z dôvodu, že Uchádzač:

· odstúpil od svojej Ponuky v čase po uplynutí lehoty na predkladanie ponúk do uplynutia lehoty viazanosti ponúk, alebo

· neposkytol súčinnosť potrebnú na uzavretie zmluvy v zmysle zákona o verejnom obstarávaní alebo

· odmietol uzavrieť zmluvu alebo rámcovú dohodu.

Komisia konštatuje, že uchádzač č. 1 Slovanet, a.s. zložil zábezpeku v súlade s § 46 ZVO a v súlade s pokynmi uvedenými v súťažných podkladoch a v stanovenej výške.

Uchádzač č. 3 SWAN, a.s. vo svojej ponuke predložil Bankovú záruku č. 626.845 zo dňa 24.01.2025 a Dodatok č. 1 k bankovej záruke č. 626.845 zo dňa 12.02.2025 vystavenú Tatra bankou, a.s.. Banková záruka je podpísaná elektronickou pečaťou TB.

Z predloženej záruky a jej dodatku vyplýva, že Banka sa zaväzuje vykonať platbu Obstarávateľovi do vyššie uvedenej sumy po predložení jeho prvej písomnej výzvy na zaplatenie, za podmienky, že Obstarávateľ v písomnej výzve na zaplatenie uvedie, že suma, ktorú požaduje, je splatná z dôvodu, že Uchádzač:

· odstúpil od svojej Ponuky v čase po uplynutí lehoty na predkladanie ponúk do uplynutia lehoty viazanosti ponúk, alebo

· neposkytol súčinnosť potrebnú na uzavretie zmluvy v zmysle zákona o verejnom obstarávaní alebo

· odmietol uzavrieť zmluvu alebo rámcovú dohodu.

Komisia konštatuje, že uchádzač č. 3 SWAN, a.s. zložil zábezpeku v súlade s § 46 ZVO a v súlade s pokynmi uvedenými v súťažných podkladoch a v stanovenej výške.

Uchádzač č. 2 Slovak Telekom, a.s. vo svojej ponuke predložil Bankovú záruku č. 2500195029 zo dňa 17.01.2025 vystavenú Komerční bankou, a.s.. Banková záruka bola predložená v listinnej podobe v lehote na predkladanie ponúk.

Z predloženej záruky a jej dodatkov č. 1 a 2 vyplýva, že Banka sa zaväzuje vykonať platbu Obstarávateľovi do vyššie uvedenej sumy po predložení písomnej výzvy na zaplatenie, ktorá bude obsahovať písomné prehlásenie, že klient v lehote viazanosti ponúk:

· odstúpil od svojej ponuky, alebo

· neposkytol súčinnosť alebo odmietol uzavrieť zmluvu alebo rámcovú dohodu podľa zákona.

Komisia konštatuje, že uchádzač č. 2 Slovak Telekom, a.s. zložil zábezpeku v súlade s § 46 ZVO a v súlade s pokynmi uvedenými v súťažných podkladoch a v stanovenej výške.

Uchádzač č. 4 O2 Business Services, a.s. vo svojej ponuke predložil Bankovú záruku č. 626.884 zo dňa 24.01.2025 a Dodatok č. 1 k bankovej záruke č. 626.884 zo dňa 12.02.2025 vystavenú Tatra bankou, a.s.. Banková záruka je podpísaná elektronickou pečaťou TB.

Z predloženej záruky a jej dodatku vyplýva, že Banka sa zaväzuje vykonať platbu Obstarávateľovi do vyššie uvedenej sumy po predložení jeho prvej písomnej výzvy na zaplatenie, za podmienky, že Obstarávateľ v písomnej výzve na zaplatenie uvedie, že suma, ktorú požaduje, je splatná z dôvodu, že Uchádzač:

· odstúpil od svojej Ponuky v čase po uplynutí lehoty na predkladanie ponúk do uplynutia lehoty viazanosti ponúk, alebo

· neposkytol súčinnosť potrebnú na uzavretie zmluvy v zmysle zákona o verejnom obstarávaní alebo

· odmietol uzavrieť zmluvu alebo rámcovú dohodu.

Komisia konštatuje, že uchádzač č. 4 O2 Business Services,, a.s. zložil zábezpeku v súlade s § 46 ZVO a v súlade s pokynmi uvedenými v súťažných podkladoch a v stanovenej výške.

Uchádzač č. 5 Antik Telekom, s.r.o. vo svojej ponuke predložil Bankovú záruku č. 626.952 zo dňa 13.02.2025 vystavenú Tatra bankou, a.s.. Banková záruka je podpísaná elektronickou pečaťou TB

Z predloženej záruky a jej dodatku vyplýva, že Banka sa zaväzuje vykonať platbu Obstarávateľovi do vyššie uvedenej sumy po predložení jeho prvej písomnej výzvy na zaplatenie, za podmienky, že Obstarávateľ v písomnej výzve na zaplatenie uvedie, že suma, ktorú požaduje, je splatná z dôvodu, že Uchádzač:

· odstúpil od svojej Ponuky v čase po uplynutí lehoty na predkladanie ponúk do uplynutia lehoty viazanosti ponúk, alebo

· neposkytol súčinnosť potrebnú na uzavretie zmluvy v zmysle zákona o verejnom obstarávaní alebo

· odmietol uzavrieť zmluvu alebo rámcovú dohodu.

Komisia konštatuje, že uchádzač č. 5 Antik Telekom, s.r.o. zložil zábezpeku v súlade s § 46 ZVO a v súlade s pokynmi uvedenými v súťažných podkladoch a v stanovenej výške.

Splnenie podmienok účasti:

Osobné postavenie - § 32 ZVO

V zmysle § 32 ZVO a časti A.2 Súťažných podkladov Podmienky účasti uchádzačov: Uchádzač musí spĺňať podmienky účasti týkajúce sa osobného postavenia uvedené v § 32 ods. 1 zákona.

Vyhodnotenie splnenia podmienky účasti podľa § 32 ZVO u uchádzača č. 1 Slovanet, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1a zápisnice č. 2 z vyhodnotenia splnenia podmienok účasti SLOVANET.

Komisia konštatuje, že uchádzač č. 1 Slovanet, a.s. splnil podmienky účasti podľa § 32 ZVO.

Vyhodnotenie splnenia podmienky účasti podľa § 32 ZVO u uchádzača č. 3 SWAN, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1b zápisnice č. 2 z vyhodnotenia splnenia podmienok účasti SWAN.

Komisia konštatuje, že uchádzač č. 3 SWAN, a.s. splnil podmienky účasti podľa § 32 ZVO.

Vyhodnotenie splnenia podmienky účasti podľa § 32 ZVO u uchádzača č. 2 Slovak Telekom, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1c zápisnice č. 2 z vyhodnotenia splnenia podmienok účasti SLOVAK TELEKOM.

Komisia konštatuje, že uchádzač č. 2 Slovak Telekom, a.s. splnil podmienky účasti podľa § 32 ZVO.

Vyhodnotenie splnenia podmienky účasti podľa § 32 ZVO u uchádzača č. 4 O2 Business Services, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1d zápisnice č. 2 z vyhodnotenia splnenia podmienok účasti O2 Business Services.

Komisia konštatuje, že uchádzač č. 4 O2 Business Services, a.s. splnil podmienky účasti podľa § 32 ZVO.

Vyhodnotenie splnenia podmienky účasti podľa § 32 ZVO u uchádzača č. 5 Antik Telekom, s.r.o. je uvedené v prílohe zápisnice DigiEDU PO Príloha č. 1e zápisnice z vyhodnotenia splnenia podmienok účasti Antik.

Finančné a ekonomické postavenie - § 33 ZVO

Nebolo požadované

Technická alebo odborná spôsobilosť - § 34 ZVO

Verejný obstarávateľ požadoval splnenie podmienok účasti podľa § 34 ods. 1 písm. a), písm. d), písm. g) a písm. j) ZVO.

Uchádzač č. 1 Slovanet, a.s.:

Vyhodnotenie splnenia podmienky účasti podľa § 34 ZVO u uchádzača č. 1 Slovanet, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1a zápisnice z vyhodnotenia splnenia podmienok účasti SLOVANET.

Komisia identifikovala zistenia v prípade preukázania splnenia podmienky účasti podľa § 34 ods. 1 písm. g) ZVO v prípade kľúčového experta č. 5 a podľa § 34 ods. 1 písm. d).

Komisia požiada uchádzača č. 1 Slovanet, a.s. o vysvetlenie k uvedeným zisteniam.

Verejný obstarávateľ dňa 21.03.2025 prostredníctvom systému na elektronickú komunikáciu JOSEPHINE v súlade s § 40 ods. 4 ZVO požiadal uchádzača o vysvetlenie k uvedeným zisteniam.

Lehota na doručenie vysvetlenia bola stanovená do 31.03.2025 do 11:00 hod.

Uchádzač č. 1 doručil vysvetlenie dňa 21.03.2025 o 15:37 hod.

Komisia konštatuje, že uchádzač č. 1 doručil vysvetlenie v stanovenej lehote.

Vo svojej odpovedi týkajúcej sa certifikátu ISO 27001 uchádzač uvádza:

„Vysvetlenie k otázke č.1

Uchádzač vo svojej ponuke predložil okrem profesijného životopisu p. Viktora Locnera súčasne dokument „Zoznam praktických skúsenosti“ p. Viktora Locnera, ktorý bol vypracovaný v súlade so štruktúrou definovanou Verejným obstarávateľom. V predmetnom Zozname skúseností sú uvedené stručné údaje o projektoch (praktických skúsenostiach), na ktorých sa navrhovaný kľúčový expert podieľal, čo možno overiť nahliadnutím do stĺpcov „Stručná charakteristika projektu“ ako aj „Pozícia na projekte a rozsah prác, ktoré vykonával a bol za ne zodpovedný“. Z daných údajov vyplýva, že p. Viktor Locner sa (okrem iných v dokumente neuvedených projektov) podieľal na aktivitách pre odberateľov:

1. Všeobecná zdravotná poisťovňa a.s.;

2. Generálna prokuratúra Slovenskej republiky;

3. Úrad pre dohľad nad zdravotnou starostlivosťou.

V rámci poskytovaných služieb pre uvedených odberateľov sú zriaďované a následne prevádzkované sieťové služby a riešenia LAN/WLAN/WAN spoločne a teda navrhovaný kľúčový expert zodpovedal a aj zodpovedá za koordináciu a implementáciu spoločných (vzájomne logicky ako aj funkčne prepojených) poskytovaných služieb LAN/WLAN/WAN. Pre vylúčenie pochybností uvádzame, že v prípade uvedeného výrazu „LAN/WLAN/WAN“, je tento potrebné interpretovať ako LAN a súčasne WLAN a súčasne WAN ako vzájomne prepojené, od seba závislé a súvisiace služby poskytované spoločne ako jedno plnenie, ktorých separátna prevádzka by „de-facto“ nebola technicky možná a udržateľná.

Uchádzač zároveň uvádza, že pri každom z uvedených plnení uviedol kontaktné údaje na zodpovednú osobu odberateľa pre účely potvrdenia uvedených informácií.

Vysvetlenie k otázke č.2

Uchádzač vo svojej ponuke predložil okrem profesijného životopisu p. Mareka Zapletala súčasne dokument „Zoznam praktických skúsenosti“ p. Mareka Zapletala, ktorý bol vypracovaný v súlade so štruktúrou definovanou Verejným obstarávateľom. V predmetnom Zozname skúseností sú uvedené stručné údaje o projektoch (praktických skúsenostiach), na ktorých sa navrhovaný kľúčový expert podieľal, čo možno overiť nahliadnutím do stĺpcov „Stručná charakteristika projektu“ ako aj „Pozícia na projekte a rozsah prác, ktoré vykonával a bol za ne zodpovedný“. Z daných údajov vyplýva, že p. Marek Zapletal sa (okrem iných v dokumente neuvedených projektov) podieľal na aktivitách pre odberateľov:

1. Všeobecná zdravotná poisťovňa a.s.;

2. Generálna prokuratúra Slovenskej republiky;

3. Úrad pre dohľad nad zdravotnou starostlivosťou.

4. Generálne riaditeľstvo zboru väzenskej a justičnej stráže

V rámci poskytovaných služieb pre uvedených odberateľov sú zriaďované a následne prevádzkované sieťové služby a riešenia LAN/WLAN/WAN spoločne a teda navrhovaný kľúčový expert zodpovedal a aj zodpovedá za koordináciu a implementáciu spoločných (vzájomne logicky ako aj funkčne prepojených) poskytovaných služieb LAN/WLAN/WAN. Pre vylúčenie pochybností uvádzame, že v prípade uvedeného výrazu „LAN/WLAN/WAN“, je tento potrebné interpretovať ako LAN a súčasne WLAN a súčasne WAN ako vzájomne prepojené, od seba závislé a súvisiace služby poskytované spoločne ako jedno plnenie, ktorých separátna prevádzka by „de-facto“ nebola technicky možná a udržateľná.

Uchádzač zároveň uvádza, že pri každom z uvedených plnení uviedol kontaktné údaje na zodpovednú osobu odberateľa pre účely potvrdenia uvedených informácii.

Vysvetlenie k otázke č.3

V prílohe tejto odpovede si Vám dovoľujeme doručiť aktuálne platný certifikát ISO 27001 s platnosťou na obdobie ďalších 3 kalendárnych rokov. Pre vysvetlenie uvádzame, že nami, v ponuke predložený certifikát

ISO 27001, bol ku dňu predkladania ponúk platný. Naša spoločnosť v období vyhodnocovania ponúk podstúpila úspešný recertifikačný cyklus na základe ktorého získala nový, ktorý kontinuálne časovo nadväzuje na pôvodný certifikát. Týmto si súčasne na základe uvedeného dovoľujeme uviesť, že podmienka účasti vo väzbe na normu ISO 27001 bola našou spoločnosťou dodržaná kontinuálne počas celej doby trvania verejného obstarávania.“

Prílohou odpovede bol certifikát o zavedení a údržby systému manažérstva informačnej bezpečnosti spĺňajúci požiadavky STN EN ISO/IEC 27001:2023 vydaný certifikačným orgánom EURO CERT group, s registračným číslom certifikátu 1755/ISMS/25 s platnosťou súčasného certifikačného cyklu od 21.2.2025 do 22.2.2028.

Vyhodnotenie splnenia podmienok účasti uchádzača č. 1 SLOVANET je uvedené v prílohe 1a zápisnice vyhodnotenie splnenia podmienok účasti SLOVANET.

Komisia konštatuje, že uchádzač č. 1 SLOVANET, a.s. IČO: 35954612 splnil podmienky účasti podľa § 34 ZVO.

Uchádzač č. 3 SWAN, a.s.:

Vyhodnotenie splnenia podmienky účasti podľa § 34 ZVO u uchádzača č. 3 SWAN, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1b zápisnice č. 2 z vyhodnotenia splnenia podmienok účasti SWAN.

Komisia konštatuje, že uchádzač č. 3 SWAN, a.s., IČO: 35680202 splnil podmienky účasti podľa § 34 ZVO.

Uchádzač č. 2 Slovak Telekom, a.s.:

Vyhodnotenie splnenia podmienky účasti podľa § 34 ZVO u uchádzača č. 2 Slovak Telekom, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1c zápisnice z vyhodnotenia splnenia podmienok účasti SLOVAK TELEKOM.

Komisia identifikovala zistenia v prípade preukázania splnenia podmienky účasti podľa § 34 ods. 1 písm. g) ZVO v prípade kľúčového experta č. 4.

Komisia požiada uchádzača č. 2 Slovak Telekom, a.s. o vysvetlenie k uvedeným zisteniam.

Verejný obstarávateľ dňa 21.03.2025 prostredníctvom systému na elektronickú komunikáciu JOSEPHINE v súlade s § 40 ods. 4 ZVO požiadal uchádzača o vysvetlenie k uvedeným zisteniam.

Lehota na doručenie vysvetlenia bola stanovená do 31.03.2025 do 11:00 hod.

Uchádzač č. 2 doručil vysvetlenie dňa 25.03.2025 o 10:00 hod.

Komisia konštatuje, že uchádzač č. 2 doručil vysvetlenie v stanovenej lehote.

Vyhodnotenie splnenia podmienok účasti uchádzača č. 2 Slovak TELEKOM je uvedené v prílohe 1a zápisnice č. 2 vyhodnotenie splnenia podmienok účasti TELEKOM.

Komisia konštatuje, že uchádzač č. 2 Slovak TELEKOM, a.s. IČO: 35763469 splnil podmienky účasti podľa § 34 ZVO.

Uchádzač č. 4 O2 Business Servicess, a.s.:

Vyhodnotenie splnenia podmienky účasti podľa § 34 ZVO u uchádzača č. 4 O2 Business Services, a.s. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1d zápisnice z vyhodnotenia splnenia podmienok účasti O2 Business Services.

Komisia identifikovala zistenia v prípade preukázania splnenia podmienky účasti podľa § 34 ods. 1 písm. g) ZVO v prípade kľúčových expertov č. 1, 2, 3, 4, 5, 7 a 9.

Komisia požiada uchádzača č. 4 O2 Business Services, a.s. o vysvetlenie k uvedeným zisteniam.

Verejný obstarávateľ dňa 21.03.2025 prostredníctvom systému na elektronickú komunikáciu JOSEPHINE v súlade s § 40 ods. 4 ZVO požiadal uchádzača o vysvetlenie k uvedeným zisteniam.

Lehota na doručenie vysvetlenia bola stanovená do 31.03.2025 do 11:00 hod.

Uchádzač č. 4 doručil vysvetlenie dňa 30.03.2025 o 22:38 hod.

Komisia konštatuje, že uchádzač č. 4 doručil vysvetlenie v stanovenej lehote.

Žiadosť o vysvetlenie sa týkala:

1. Vysvetlenie alebo doplnenie predložených dokladov pre Experta č. 1 týkajúcich sa preukázania praktických skúseností

2. Vysvetlenie alebo doplnenie predložených dokladov pre Experta č. 4 pre účely posúdenia splnenia podmienky účasti

3. Vysvetlenie alebo doplnenie predložených dokladov pre Experta č. 5 pre účely posúdenia splnenia podmienky účasti

4. Vysvetlenie alebo doplnenie predložených dokladov – úradne overených prekladov – Expertov č. 1, 2, 3, 4, 7 a 9

5. Vysvetlenie alebo doplnenie predložených dokladov pre Experta č. 9 pre účely posúdenia splnenia podmienky účasti

6. Vysvetlenie alebo doplnenie predložených dokladov pre inú osobu O2 Slovakia, s.r.o. pre účely posúdenia splnenia podmienky účasti

Okrem iných dokladov uchádzač vo svojej odpovedi v prípade kľúčového experta č. 9 predložil certifikáty PRINCE2 Project Management a ITIL Foundation Certificate in IT Service Management.

Podľa súťažných podkladov časti A.2 Podmienky účasti, u kľúčového experta č. 9 verejný obstarávateľ požadoval:

„Expert č.9 na pozícii Špecialista pre Service desk – senior (minimálne 1 osoba)

a) minimálne 3-ročnú odbornú prax v pozícii NOC (Network Operations Center) manažéra alebo ServiceDesk manažéra,

b) minimálne 1 praktická skúsenosť na pozícii manažéra v oblasti riadenia NOC/ ServiceDesk a riadenia kvality služieb,

c) expert je držiteľom certifikátu ITIL Foundation alebo vyššia úroveň pre preukázanie znalostí v oblasti riadenia IT služieb (alebo ekvivalent).

Jednotlivé čiastkové podmienky účasti na expertov sa preukazujú nasledovným spôsobom:

- *podmienka na odbornú prax sa preukazuje vlastnoručne podpísaným profesijným životopisom alebo ekvivalent (sken),*
- *podmienka na praktické skúsenosti sa preukazuje vlastnoručne podpísaným zoznamom praktických skúseností experta (sken),*
- *podmienka na certifikát alebo osvedčenie sa preukazuje skenom platného certifikátu alebo osvedčenia.“*

Nakoľko verejný obstarávateľ nepožadoval splnenie podmienky účasti u experta č. 9 vydaním certifikátu PRINCE2, komisia sa nebude zaoberať predloženým dokladom – PRINCE2 Foundation Certificate in Project Management, vydaného PepopleCert a Axelos global best practice účinný od 17.01.2020, číslo certifikátu GR633128617MK, číslo kandidáta: 9980034014421371 s dobou účinnosti uvedenou: „N/A“.

Kontrolou certifikátu kľúčového experta č. 9 ITIL Foundation Certificate in IT Service Management, vydaného PepopleCert a Axelos global best practice účinný od 24.01.2020, číslo certifikátu GR671118780MK, číslo kandidáta: 9980034014421371 s dobou účinnosti uvedenou: „N/A“ komisia zistila nasledovné: kontrolou na stránke https://www.microcomp.sk/aktuality-detail/koniec-neobmedzenej-platnosti-certifikatov-peoplecert-axelos bolo zistené:

„Celosvetová komunita pre Global Best Practice PeopleCert - AXELOS zverejnila nové podmienky vydávania certifikátov. Táto zmena platí od 1. 1. 2023 aj pre certifikácie uskutočnené v minulosti. K tomuto kroku sa

PeopleCert rozhodol kvôli spusteniu nového programu pre kontinuálny profesný rozvoj (Continuing Professional Development - CPD), ktorý má pomôcť udržať si náskok v konkurencii na trhu práce.

Všetci kandidáti s certifikátom PeopleCert Global Best Practice sa môžu rozhodnúť pre obnovu do troch rokov od pôvodného dátumu certifikácie. Tí, ktorí boli certifikovaní pred 30. 6. 2020 majú platnosť certifikátom do 1. 7. 2023 a to bez ohľadu na pôvodný dátum udelenia.

Niektoré certifikáty, napr. PRINCE2® verzia 5. a 6. už boli vydávané s platnosťou na 3 roky aj v minulosti. Avšak boli aj také, ako napr. ITIL, ktoré boli vydávané s neobmedzenou platnosťou na danú verziu, aktuálne ITIL 4.“

Zmena platnosti na 3 roky s možnosťou obnovenia platí aj pre certifikát ITIL4.

Zároveň, verejný obstarávateľ pristúpil k overeniu predmetného certifikátu z číslom GR671118780MK prostredníctvom verifikačnej služby pre certifikáciu spoločnosti PeopleCert ktorá certifikát vydala,

(https://www.peoplecert.org/for-corporations/certificate-verification-service), s výsledkom overenia *„Táto certifikácia si vyžaduje obnovenie, aby zodpovedala aktuálnym certifikačným požiadavkám“* (viď príloha 3 zápisnice z vyhodnotenia podmienok účasti O2BS ITIL).

Vo vysvetlení uchádzač uvádza:
„V priebehu času platnosti certifikátu však došlo k zmene podmienky certifikácie a bola zavedená obmedzená doba platnosti certifikátu, a to aj spätne pre už vydané certifikáty, pričom táto skutočnosť nastala aj z dôvodu majetkovej zmeny v rámci certifikačnej autority, kedy nový majiteľ zmenil jednostranne podmienky. Spoločnosť PeopleCert International Ltd. kúpila značku trademark ITIL a následne jednostranne zmenila podmienky, a zároveň porušila jej základnú povinnosť akýmkoľvek spôsobom informovať o tejto zmene držiteľov platných certifikátov. Naša spoločnosť zamestnáva ďalších troch expertov, ktorí získali časovo neobmedzený ITIL Foundation certifikát, pričom ani jeden z nich nebol o zmene pravidiel informovaný.
Uchádzač bol týmto aktom bez vlastného zavinenia uvedený do omylu treťou stranou, ktorá ako jediná na svete rozhoduje o ITIL certifikácii.
Ako bolo spomenuté vyššie, o tejto skutočnosti p. Kubiková nebola riadne upovedomená zo strany certifikačnej autority a z tohto dôvodu si nebola vedomá potreby jeho obnovenia. Zároveň uvádzame, že podľa dostupných informácií takéto upovedomenie nebolo doručené žiadnej osobe, ktorá týmto certifikátom disponovala alebo disponuje. Preto bol certifikát Experta č. 9 predložený v našej ponuke, pričom v čase predkladania ponuky sme mali za to, že predmetný certifikát je platný. Zároveň uvádzame, že Expert č. 9 reálne disponuje skúsenosťami, ktoré sú spojené s požadovanou ITIL certifikáciou a činnosti, ktoré by táto osoba mala zastávať v Zákazke reálne aj teraz vykonáva. V rámci zabezpečenia súladu s požiadavkami Verejného obstarávateľa a súťažnými podkladmi uvádzame, že Expertka č. 9 – p. Kubiková si platnosť požadovaného certifikátu pre Experta č. 9 k dnešnému dňu obnovila, a zároveň predkladáme aktualizovaný certifikát aj s jeho úradným prekladom.“

Prílohou odpovede bol, okrem iných požadovaných dokladov, aj úradný preklad certifikátu ITIL Foundation certificate in IT Servise Management vydaný na meno Martina Kubikova, číslo certifikátu GR671762121MK s platnosťou od 07.04.2025 do 07.04.2028.

Komisia doplnenie vysvetlenia akceptuje a konštatuje, že uchádzač splnil podmienku účasti týkajúcu sa kľúčového experta č. 9 na pozícii Špecialista pre Service desk – senior.

Vyhodnotenie splnenia podmienok účasti uchádzača č. 4 O2 Business Services je uvedené v prílohe 1a zápisnice č. 2 vyhodnotenie splnenia podmienok účasti O2 BS.

Komisia konštatuje, že uchádzač č. 4 O2 Business Services, a.s. IČO: 50087487 splnil podmienky účasti podľa § 34 ZVO.

Uchádzač č. 5 Antik Telekom, s.r.o.:

Vyhodnotenie splnenia podmienky účasti podľa § 34 ZVO u uchádzača č. 5 Antik Telekom, s.r.o. je uvedené v prílohe zápisnice DigiEDU NR Príloha č. 1e zápisnice z vyhodnotenia splnenia podmienok účasti Antik.

Komisia identifikovala zistenia v prípade preukázania splnenia podmienky účasti podľa § 34 ods. 1 písm. d) ZVO v prípade platného certifikátu o zavedení systému manažérstva informačnej bezpečnosti podľa normy ISO 27001 v oblasti IKT, vydaného nezávislou inštitúciou. Pričom uchádzač mohol využiť systémy manažérstva informačnej bezpečnosti v oblasti informačných systémov vyplývajúce z európskych noriem. Verejný obstarávateľ zároveň uzná ako rovnocenné osvedčenia vydané príslušnými orgánmi členských štátov.

Komisia požiada uchádzača č. 5 Antil Telekom, s.r.o. o vysvetlenie k uvedeným zisteniam.

Verejný obstarávateľ dňa 21.03.2025 prostredníctvom systému na elektronickú komunikáciu JOSEPHINE v súlade s § 40 ods. 4 ZVO požiadal uchádzača o vysvetlenie k uvedeným zisteniam.

Lehota na doručenie vysvetlenia bola stanovená do 31.03.2025 do 10:00 hod.

Uchádzač č. 5 doručil vysvetlenie dňa 31.03.2025 o 10:56 hod.

Komisia konštatuje, že uchádzač č. 5 Antik Telekom, s.r.o. doručil vysvetlenie v stanovenej lehote.

Vo svojej odpovedi uchýdzač č. 5 uviedol:

,,na základe žiadosti o vysvetlenie podľa § 40ods. 4 ZVO si Vám dovoľujeme zaslať nasledovné vyjadrenie:

1. A) Uchádzač predkladá doklad o preukázaní k ekvivalentnosti vykonávanému auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z. v našej spoločnosti k norme ISO 27001 v oblasti IKT.

B) V Dokumente „Potvrdenie o vykonaní auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z.“ bolo chybne uvedené číslo registrovaného subjektu, jednalo sa o chybu v písaní na strane p. Mareka Uličného. V Prílohe zasielame dokument: Potvrdenie o vykonaní auditu kybernetickej bezpečnosti podpísaný p. Marekom Uličným s uvedením opraveného evidenčného čísla certifikátu audítora.

2. Uchádzač predkladá dokument: Čestné vyhlásenie k splneniu podmienky účasti podľa § 34 ods. 1 písm. j) ZVO, ktorý sme z dôvodu administratívnej chyby opomenuli pripojiť k predchádzajúcej odpovedi. Vzhľadom na to, že sme doklady nahradili JED formulárom túto podmienku účasti spĺňame k termínu podania cenovej ponuky.“

Po vyhodnotení predložených dokumentov komisia konštatovala, že z predložených dokladov nie je možné jednoznačne posúdiť splnenie podmienky účasti podľa § 34 ods. 1 písm. d) ZVO a z uvedeného dôvodu dňa 06.06.2025 opakovane požiadala uchádzača č. 5 o predloženie vysvetlenia.

Lehota na doručenie vysvetlenia bola stanovená do 16.06.2025 do 14:00 hod.

Žiadosť o vysvetlenie č. 2 sa týkala:

Verejný obstarávateľ v rámci Súťažných podkladov časť A.2 Podmienky účasti v súlade s § 34 ods. písm. d) zákona ZVO stanovil, za účelom preukázania technickej alebo odbornej spôsobilosti uchádzača, minimálnu požadovanú úroveň štandardov a doklady a dokumenty, ktorými uchádzač preukazuje splnenie podmienok účasti týkajúce sa technickej alebo odbornej spôsobilosti podľa § 34 ods. 1 písm. d) zákona nasledovne:

> Platný certifikát o zavedení systému manažérstva informačnej bezpečnosti podľa normy **ISO 27001** v oblasti IKT, vydaný nezávislou inštitúciou. Uchádzač môže využiť systémy manažérstva informačnej bezpečnosti v oblasti informačných systémov vyplývajúce z európskych noriem. Verejný obstarávateľ uzná ako rovnocenné osvedčenia vydané príslušnými orgánmi členských štátov

Uchádzač predložil doklad *„Potvrdenie o vykonaní auditu kybernetickej bezpečnosti podľa z.69/2018 Z.z.SR“* vydané dňa 26.2.2025 spoločnosťou IT ASSISTANCE, s.r.o. – podpísaný Marekom Uličným (ďalej len „potvrdenie“).

V uvedenom potvrdení sa uvádza:

„ Spoločnosť ANTIK Telecom s.r.o., IČO 36 191 400, je regulovaným subjektom podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov a pravidelne, v dvojročnom cykle

vykonáva nezávislý audit súladu s týmto zákonom, ktorý spĺňa atribúty systému manažérstva informačnej bezpečnosti podľa normy ISO 27001 v oblasti IKT.

Posledný audit súladu s požiadavkami zákona č. 68/2018 Z. z. o kybernetickej bezpečnosti bol nami vykonaný v apríli 2023.“

Z uvedeného potvrdenia však nebolo možné jednoznačne posúdiť splnenie predmetnej podmienky účasti, a to konkrétne:

a) Či uchádzač disponuje platným certifikátom o zavedení systému manažérstva informačnej bezpečnosti podľa normy ISO 27001 v oblasti IKT, vydaným nezávislou inštitúciou,
b) Či vykonaný audit kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. spĺňa atribúty systému manažérstva informačnej bezpečnosti podľa normy ISO 27001 v oblasti IKT, pričom toto tvrdenie nebolo podložené relevantnými dôkazmi.

Preto, na základe vyššie uvedených zistení, verejný obstarávateľ dňa 21.03.2025 vyzval uchádzača prostredníctvom Žiadosti o vysvetlenie, aby v stanovenej lehote (do 31.03.2025 do 11:00 hod.) predložil vysvetlenie a/alebo relevantné doklady, ktoré jednoznačne preukazujú splnenie uvedenej podmienky účasti, a to:

- pre potreby preukázania ekvivalentnosti, vyzýva uchádzača, aby uchádzač v štruktúrovanej forme preukázal, že vykonaný audit kybernetickej bezpečnosti podľa zákona č. 69/2018 Z. z. obsahuje všetky prvky manažérstva informačnej bezpečnosti podľa normy ISO 27001 v oblasti IKT, ktoré verejný obstarávateľ preukázaním normy ISO 27001 v oblasti IKT vyžadoval v podmienkach účasti.
- v predloženom dokumente *„Potvrdenie o vykonaní auditu kybernetickej bezpečnosti podľa z.69/2018 Z.z.SR“* vydané dňa 26.2.2025 spoločnosťou IT ASSISTANCE, s.r.o. podpísané Marekom Uličným“ je:
    - „pečiatka“ SNAS Reg. No. 695/O-024 je číslo registrovaného subjektu v SNAS – konkrétne Kompetenčné a certifikačné centrum kybernetickej bezpečnosti (štátna príspevková organizácia zriadená zakladateľskou listinou, zriaďovateľ NBÚ). Toto registračné číslo nijak nesúvisí s osobou p. Marek Uličný a ani so spoločnosťou IT ASSISTANCE s.r.o.
    - Certifikát vydaný na osobu p. Ing. Marek Uličný – je vydaný na osobu, nie na spoločnosť IT ASSISTANCE, s.r.o., preto akékoľvek prehlásenie vydané touto osobou nie je vo vzťahu k IT ASSISTANCE, s.r.o. ako certifikovanému subjektu, ktorým je p. Marek Uličný.

Uchádzač v stanovenej lehote (dňa 31.03.2025 o 10:56 hod.) doručil odpoveď na Žiadosť o vysvetlenie, v rámci ktorej poskytol:

1. A) doklad o preukázaní k ekvivalentnosti vykonávanému auditu kybernetickej bezpečnosti podľa zákona č.69/2018 Z.z. v našej spoločnosti k norme ISO 27001 v oblasti IKT,
Dokument s názvom *System manazerstva informacnej bezpecnosti v spolocnosti ANTIK Telecom s.r.o..pdf, zo dňa 28.03.2025, ktorý vypracoval p.Oliver Nemčik, Manažér Kybernetickej bezpečnosti, Antik Telecom s.r.o.*

1. B) Vysvetlenie týkajúce sa Dokumentu „Potvrdenie o vykonaní auditu kybernetickej bezpečnosti podľa zákona č. 69/2018 Z.z.“ cit. *„bolo chybne uvedené číslo registrovaného subjektu, jednalo sa o chybu v písaní na strane p. Mareka Uličného. V Prílohe zasielame dokument: Potvrdenie o vykonaní auditu kybernetickej bezpečnosti podpísaný p. Marekom Uličným s uvedením opraveného evidenčného čísla certifikátu audítora.“*

2. dokument: Čestné vyhlásenie k splneniu podmienky účasti podľa § 34 ods. 1. písm. j) ZVO, cit „*ktorý z dôvodu administratívnej chyby opomenul pripojiť k predchádzajúcej odpovedi. Vzhľadom na to, že sme doklady nahradili JED formulárom túto podmienku účasti spĺňame k termínu podania cenovej ponuky.“*

Ku svojej odpovedi uchádzač priložil dokumenty:

- Čestné vyhlásenie k splneniu technickej a odbornej spôsobilosti
- Systém manažérstva informačnej bezpečnosti v spoločnosti ANTIK Telekom, s.r.o.

V rámci dokumentu (1.A) *System manazerstva informacnej bezpecnosti v spolocnosti ANTIK Telecom s.r.o..pdf, zo dňa 28.03.2025, ktorý vypracoval p.Oliver Nemčik, Manažér Kybernetickej bezpečnosti, Antik Telecom s.r.o. (ďalej len **„Systém manažérstva IB“**) uchádzač prehlásil v úvode, že zaviedol systém manažérstva informačnej bezpečnosti (ISMS)v súlade so zákonom 69/2018 Z.z. a nemu prislúchajúcej Vyhláške č.362/2018. Zároveň uviedol predstavenie hlavných požiadaviek normy ISO 27001.*

Uchádzač uviedol v Kapitole 3 „Porovnanie s normou ISO/IEC 27002“ jednotlivé kapitoly normy a kým spôsobom ich uchádzač implementoval v jeho vlastnom ISMS.

Pre úplnosť poznamenávame, že Norma ISO/IEC 27001:2013 obsahuje 114 kontrolných opatrení, uvedených v jej prílohe (Annex A), pričom norma ISO/IEC 27002 je technickým usmernením (code of practice), ktoré podrobne rozpracováva a vysvetľuje opatrenia uvedené v prílohe A normy ISO/IEC 27001 (ďalej len „norma“) – viď príloha tejto žiadosti o vysvetlenie.

Komisia verejného obstarávateľa porovnala skupiny kontrolných opatrení uvedených v prílohe A Normy ISO/IEC 27001:2013 s odpoveďami uvedenými v odpovedi uchádzača na žiadosť o vysvetlenie zo dňa 31.03.2025 bode 3 – Porovnanie s normou ISO/IEC 27002:

1. Politika informačnej bezpečnosti

Vo svojej odpovedi uchádzač uvádza:

> Naša organizácia vypracovala a prijala politiku informačnej bezpečnosti, ktorá stanovuje základné princípy a ciele na ochranu informačných aktív. Táto politika je schválená vrcholovým vedením a je pravidelne revidovaná.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

A.5 — Information Security Policies

- **Úloha:** Dokumentovanie pravidiel a politík pre riadenie informačnej bezpečnosti
- Podkategórie:
  - A.5.1.1 – Dokument o politike informačnej bezpečnosti

Komisia konštatuje splnenie požiadavky normy ISO/IEC 27001 na vypracovanie dokumentu o politike informačnej bezpečnosti.

2. Organizácia informačnej bezpečnosti

Vo svojej odpovedi uchádzač uvádza:

> V rámci našej organizácie sme zaviedli jasné organizačné štruktúry a zodpovednosti pre riadenie informačnej bezpečnosti. Vymenovali sme manažéra kybernetickej bezpečnosti, Olivera Nemčíka, ktorý je zodpovedný za implementáciu a dohľad nad ISMS.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

V rámci normy je definovaná kategória A.6 a jej 5 podkategórií.

A.6 — Organization of Information Security

- **Úloha:** Definovanie úloh, zodpovedností a komunikácie v bezpečnosti

- Podkategórie:
    - A.6.1.1 – Úlohy a zodpovednosti
    - A.6.1.2 – Oddelenie povinností
    - A.6.1.3 – Kontakt s orgánmi
    - A.6.1.4 – Kontakt so záujmovými skupinami
    - A.6.1.5 – Bezpečnosť v riadení projektov

Otázka č.1

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.6.1.2, A.6.1.3, A.6.1.4 a A.6.1.5, vzhľadom na skutočnosť, že uchádzač neuviedol popis tejto kategórie A.6 a jej podkategórií (A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4 a A.6.1.5) v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

Otázka č.2

V rámci normy je definovaná kategória A.7 a jej 4 podkategórie.

A.7 — Human Resource Security

- **Úloha:** Zabezpečiť, aby zamestnanci a spolupracovníci boli dôveryhodní a informovaní
- Podkategórie:
    - A.7.1.1 – Preverovanie (background check)
    - A.7.1.2 – Podmienky zamestnania
    - A.7.2.2 – Povedomie, školenia a vzdelávanie
    - A.7.2.3 – Disciplinárne konanie

Pre overenie ekvivalentnosti ISMS uchádzača, vzhľadom na skutočnosť, že uchádzač neuviedol popis tejto kategórie A.7 a jej podkategórií (A.7.1.1, A.7.1.2, A.7.2.2, A.7.2.3) v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***., žiadame o vysvetlenie o vysvetlenie akým spôsobom sú implementované v ISMS uchádzača.

3. Riadenie aktív

Vo svojej odpovedi uchádzač uvádza:

> Zaviedli sme systém riadenia aktív, ktorý zahŕňa identifikáciu, inventarizáciu a klasifikáciu informačných aktív. Tieto aktíva sú pravidelne monitorované a hodnotené z hľadiska rizík.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

V rámci normy je pre riadenie aktív definovaná kategória A.8 a jej 6 podkategórii.

A.8 — Asset Management

- **Úloha:** Správa aktív, ich vlastníctvo a správne používanie
- Podkategórie:
    - A.8.1.1 – Inventarizácia aktív
    - A.8.1.2 – Vlastníctvo aktív
    - A.8.1.3 – Prijateľné používanie aktív
    - A.8.2.1 – Klasifikácia informácií
    - A.8.2.2 – Označovanie informácií

- A.8.2.3 – Zaobchádzanie s aktívami

Otázka č.3

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.8 (A.8.1.2, A.8.1.3, A.8.2.3), vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

4. Riadenie prístupu

Vo svojej odpovedi uchádzač uvádza:

> Naša organizácia má zavedené kontrolné mechanizmy na riadenie prístupu k informačným systémom a aktívam. Tieto mechanizmy zahŕňajú autentifikáciu, autorizáciu a kontrolu prístupových práv.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

V rámci normy je definovaná kategória A.9 a jej 7 podkategórii

A.9 — Access Control

- **Úloha:** Riadenie prístupu používateľov k informačným systémom
- Podkategórie:
  - A.9.1.1 – Politika riadenia prístupu
  - A.9.2.1 až A.9.2.5 – Registrácia, poskytovanie, riadenie a revízia prístupu
  - A.9.3.1 – Používanie tajných autentifikačných údajov

Otázka č.4

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.9 (A.9.1.1, A.9.2.1 až A.9.2.5 a A.9.3.1), vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

5. **Kryptografia**

Vo svojej odpovedi uchádzač uvádza:

> Používame moderné kryptografické metódy na ochranu citlivých informácií. Kryptografické postupy sú pravidelne testované a aktualizované podľa najnovších bezpečnostných štandardov.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

A.10 — Cryptography

- **Úloha:** Používanie kryptografie na ochranu informácií
- Podkategórie:
  - A.10.1.1 – Kryptografické opatrenia

Komisia konštatuje splnenie požiadavky normy ISO/IEC 27001 na zavedenie kryptografických opatrení.

6. **Fyzická a environmentálna bezpečnosť**

Vo svojej odpovedi uchádzač uvádza:

> Zabezpečili sme fyzickú ochranu našich informačných systémov a aktív prostredníctvom kontrol prístupu, ochranných opatrení proti požiarom a klimatických podmienok.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

V rámci normy je definovaná kategória A.11 a jej 12 podkategórii.

A.11 — Physical and Environmental Security

- **Úloha:** Ochrana fyzických zariadení a priestorov
- Podkategórie:
  - A.11.1.1 až A.11.1.6 – Fyzická bezpečnostná hranica, kontrola vstupu, ochrana kancelárií, ochrana pred vonkajšími hrozbami, zabezpečenie práce v zabezpečených oblastiach, oblasť dodávok
  - A.11.2.1 až A.11.2.6 – Ochrana a údržba zariadení, káblovanie, bezpečné likvidovanie aktív

Otázka č.5

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.11.2.1 až A.11.2.6, vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

7. **Bezpečnosť prevádzky**

Vo svojej odpovedi uchádzač uvádza:
Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

> Zaviedli sme bezpečnostné opatrenia na ochranu informačných systémov počas ich prevádzky. Tieto opatrenia zahŕňajú monitorovanie systémov, zálohovanie dát a riadenie incidentov.

V rámci normy je definovaná kategória A.12 a jej 13 podkategórii

A.12 — Operations Security

- **Úloha:** Prevádzkové bezpečnostné opatrenia a kontroly
- Podkategórie:
  - A.12.1.1 až A.12.1.4 – Prevádzkové postupy, riadenie zmien, kapacity, akceptácia systému
  - A.12.2.1 – Opatrenia proti škodlivému softvéru
  - A.12.3.1 – Zálohovanie
  - A.12.4.1 až A.12.4.4 – Zaznamenávanie udalostí, ochrana logov, synchronizácia času
  - A.12.5.1 – Inštalácia softvéru na produkčné systémy
  - A.12.6.1 – Riadenie technických zraniteľností
  - A.12.7.1 – Kontroly auditov IS

Otázka č.6

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.12 (A.12.1.1 až A.12.1.4, A.12.2.1, A.12.3.1, A.12.4.1 až A.12.4.4, A.12.5.1 , A.12.6.1, A.12.7.1), vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

8. **Bezpečnosť komunikácií**

Vo svojej odpovedi uchádzač uvádza:

Naša organizácia zabezpečuje bezpečnosť komunikácií prostredníctvom šifrovania dát a kontrol prístupu k sieťovým systémom. Komunikácie sú monitorované na prítomnosť bezpečnostných hrozieb.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:

V rámci normy je definovaná kategória A.13 a jej 6 podkategórii

A.13 — Communications Security

- **Úloha:** Ochrana informačných tokov a sieťových služieb
- Podkategórie:
  - A.13.1.1 – Kontroly siete
  - A.13.1.2 – Bezpečnosť sieťových služieb
  - A.13.2.1 až A.13.2.4 – Politiky prenosu informácií, dohody, elektronická komunikácia, dohody o mlčanlivosti

Otázka č.7

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.13 (A.13.1.1, A.13.1.2, A.13.2.1 až A.13.2.4), vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

9. **Akvizícia, vývoj a údržba systémov**

Vo svojej odpovedi uchádzač uvádza:

Pri akvizícii, vývoji a údržbe informačných systémov dodržiavame bezpečnostné štandardy a postupy. Zohľadňujeme bezpečnostné riziká od začiatku vývojového procesu až po údržbu systémov.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:
V rámci normy je definovaná kategória A.14 a jej 10 podkategórii

A.14 — System Acquisition, Development and Maintenance

- **Úloha:** Zaistenie bezpečnosti pri vývoji a údržbe systémov
- Podkategórie:
  - A.14.1.1 – Analýza a špecifikácia bezpečnostných požiadaviek
  - A.14.2.1 až A.14.2.9 – Politika bezpečného vývoja, riadenie zmien, technické kontroly, bezpečný vývoj, outsourcing, testovanie bezpečnosti a akceptácie

Otázka č.8

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.14 (A.14.1.1, A.14.2.1 až A.14.2.9), vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

Otázka č.9

V rámci normy je definovaná kategória A.15 a jej 4 podkategórie

A.15 — Supplier Relationships

- ***Úloha:*** *Riadenie bezpečnosti vo vzťahoch s dodávateľmi*
- *Podkategórie:*
  - *A.15.1.1 a A.15.1.2 – Bezpečnosť a zmluvy s dodávateľmi*
  - *A.15.2.1 a A.15.2.2 – Monitorovanie a riadenie zmien služieb dodávateľov*

Otázka č. 9

Pre overenie ekvivalentnosti ISMS uchádzača, vzhľadom na skutočnosť, že uchádzač neuviedol popis tejto kategórie A.15 a jej podkategórií (A.15.1.1, A.15.1.2, A.15.2.1, A.15.2.2) v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***., žiadame o vysvetlenie akým spôsobom sú implementované v ISMS uchádzača.

10. **Riadenie incidentov informačnej bezpečnosti**

Vo svojej odpovedi uchádzač uvádza:

Máme zavedené procesy na riadenie incidentov informačnej bezpečnosti, ktoré zahŕňajú detekciu, reakciu a obnovu po incidente. Incidenty sú dokumentované a analyzované na zlepšenie bezpečnostných opatrení.

Zaradenie kontrolného opatrenia podľa prílohy normy ISO/IEC 27001:2013:
V rámci normy je definovaná kategória A.16 a jej 6 podkategórii

A.16 — Information Security Incident Management

- ***Úloha:*** *Riadenie bezpečnostných incidentov*
- *Podkategórie:*
  - *A.16.1.1 až A.16.1.6 – Riadenie, hlásenie, posudzovanie, reakcia, a poučenie sa z incidentov*

Otázka č.10

Pre overenie ekvivalentnosti ISMS uchádzača, žiadame o vysvetlenie akým spôsobom uchádzač implementoval vo svojom ISMS podkategórie normy A.16 (A.16.1.1 až A.16.1.6), vzhľadom na skutočnosť, že uchádzač neuviedol popis týchto podkategórií v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***.

Otázka č.11

V rámci normy je definovaná kategória A.17 a jej 2 podkategórie

11. **Aspekty informačnej bezpečnosti a Biznis Continuity management *A.17 — Information Security Aspects of Business Continuity Management***

- ***Úloha:*** *Zaistenie kontinuity bezpečnosti informácií v krízových situáciách*
- *Podkategórie:*
  - *A.17.1.1 – Kontinuita informačnej bezpečnosti*
  - *A.17.1.2 – Redundancie*

Pre overenie ekvivalentnosti ISMS uchádzača, vzhľadom na skutočnosť, že uchádzač neuviedol popis tejto kategórie A.17 a jej podkategórií (A.17.1.1, A.17.1.2) v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***., žiadame o vysvetlenie akým spôsobom sú implementované v ISMS uchádzača.

Otázka č.12

V rámci normy je definovaná kategória A.18 a jej 5 podkategórii

A.18 — Compliance

- ***Úloha:*** *Dodržiavanie zákonov, práv a noriem*
- *Podkategórie:*
    - *A.18.1.1 až A.18.1.5 – Identifikácia legislatívy, ochrana práv duševného vlastníctva, ochrana záznamov, ochrana osobných údajov, regulácia kryptografie*

Pre overenie ekvivalentnosti ISMS uchádzača, vzhľadom na skutočnosť, že uchádzač neuviedol popis tejto kategórie A.18 a jej podkategórií (A.18.1.1, A.18.1.5) v Kapitole 3 predloženého dokumentu ***Systém manažérstva IB***., žiadame o vysvetlenie akým spôsobom sú implementované v ISMS uchádzača.

Otázka č. 13:

Uchádzač vo svojej odpovedi v bode 5. Potvrdenie o vykonaní auditu kybernetickej bezpečnosti predložil Potvrdenie o vykonávaní auditu kybernetickej bezpečnosti vydané p. Marekom Uličným, certifikovaným audítorom kybernetickej bezpečnosti zo dňa 31.03.2025, v ktorom uvádza, že uchádzač je regulovaným subjektom podľa zákona č. 69/2018 Z.z. Zákon o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.

Podľa zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti je audit kybernetickej bezpečnosti definovaný ako systematický, nezávislý a dokladovo overiteľný proces hodnotenia úrovne ochrany informačných systémov.
Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti ukladá povinným subjektom (najmä prevádzkovateľom základných služieb) vykonávať audit kybernetickej bezpečnosti. Tento audit overuje, či organizácia splnila všetky požiadavky zákona a súvisiacich predpisov (najmä vyhlášky NBÚ č. 362/2018 Z.z.) a či zavedené bezpečnostné opatrenia zodpovedajú stanoveným kritériám. Cieľom auditu je dosiahnuť požadovanú úroveň ochrany pred kybernetickými incidentmi – identifikovať nedostatky a prijať opatrenia na ich nápravu s cieľom predchádzať bezpečnostným incidentom.
Výsledkom auditu je auditná správa, ktorá má podľa vyhlášky NBÚ stanovenú štruktúru. Obsahuje úvod (identifikáciu auditu, kto ho vykonal, kedy, koho auditoval), rozsah auditu (ktoré siete a IS boli hodnotené), zistenia auditu – zvyčajne formou prehľadnej tabuľky alebo odsekov pre každú oblasť, a záver auditu. Súčasťou správy je aj sumár zhôd a nezhôd (napr. počet zistených čiastočných a úplných nesúladov), vyhodnotenie efektívnosti opatrení a identifikované riziká.

Uchádzačom predložené Potvrdenie o vykonaní auditu Kybernetickej bezpečnosti neobsahuje informáciu o rozsahu auditu, jeho zisteniach a o závere auditu a o odovzdaní auditnej správy na NBÚ.

V zmysle vyššie uvedeného žiadame o vysvetlenie/doplnenie absentujúcich informácií.

Otázka č. 14:

Uchádzač vo svojej odpovedi v bode 5. Potvrdenie o vykonaní auditu kybernetickej bezpečnosti uvádza, že posledný audit bol vykonaný v apríli 2023.

Podľa § 20 ods. 1 zákona č. 69/2018 Z.z. je prevádzkovateľ základnej služby povinný zabezpečiť vykonanie auditu kybernetickej bezpečnosti najmenej raz za dva roky. Vyhláška NBÚ č. 362/2018 Z.z., ktorá upravuje podrobnosti o audite, tento interval potvrdzuje a špecifikuje aj požiadavky na obsah, rozsah a vykonávateľa auditu.

a) Žiadame uchádzača o vysvetlenie, či ku ukončeniu dvojročného obdobia od vykonania posledného auditu kybernetickej bezpečnosti v apríli 2023 bol vykonaný audit kybernetickej bezpečnosti podľa § 20 ods. 1 zákona č. 69/2018 Z.z a vyhlášky NBÚ č. 362/2018 Z.z.

b) Žiadame o predloženie dôkazov o vykonanom audite kybernetickej bezpečnosti s uvedením jeho rozsahu, zisteniach a o záveroch auditu s uvedením dátumu vypracovania auditnej správy a dátumu jej odovzdania na NBÚ.

Otázka č. 15:

Uchádzač vo svojej odpovedi predložil dokument s názvom „System manazerstva informacnej bezpecnosti v spolocnosti ANTIK Telecom s.r.o..pdf“, zo dňa 28.03.2025, ktorý vypracoval p.Oliver Nemčik, Manažér Kybernetickej bezpečnosti, Antik Telecom s.r.o..
Predložený dokument má v záhlaví uvedené: „Systému manažérstva informačnej bezpečnosti v spoločnosti ANTIK Telecom, s.r.o.“.

V bode 1. Úvod je uvedené: „Tento dokument slúži ako dôkaz o implementácii ISMS a jeho porovnanie s ISO/IEC 27002, ktoré je implementačnou normou pre súlad s ISO/IEC 27001.“

Nakoľko z uvedeného obsahu predmetného dokumentu nie je zrejmé, či sa jedná o samotný dokument ISMS (vychádzajúc z názvu dokumentu), alebo ide o opis potvrdzujúci implementáciu systému ISMS žiadame o vysvetlenie uvedeného zistenia.

Otázka č. 16:

Komisia má za to, že dokument je kľúčovým nástrojom pre implementáciu a riadenie bezpečnosti informácií v organizácii, čo vo svojej odpovedi potvrdzuje aj uchádzač.

Implementácia ISMS je proces, ktorý vyžaduje angažovanosť a podporu na všetkých úrovniach organizácie. Tento proces je zameraný na zabezpečenie systémov, procesov a ľudí, ktorí sú zodpovední za ochranu citlivých informácií. Postup pri prijímaní ISMS zahŕňa niekoľko kľúčových krokov a fáz, pričom na schválení a podporovaní ISMS sa podieľa vedenie organizácie.

Žiadame o preukázanie oficiálneho/formálneho schválenia finálnych dokumentov ISMS vedením organizácie formou kópií (skenov) dokumentov zahŕňajúcich minimálne:

- Prehľad a potvrdenie cieľov ISMS: dokument/doklad, v ktorom vedenie uchádzača potvrdilo, že ISMS plne zodpovedá obchodným potrebám organizácie, bezpečnostným požiadavkám a predpisom.
- Potvrdenie riadenia rizík: dokument/doklad, v ktorom vedenie uchádzača potvrdilo, že všetky identifikované riziká boli riadne vyhodnotené a že potrebné opatrenia boli implementované.
- Záväzok k neustálemu zlepšovaniu: dokument/doklad, v ktorom vedenie uchádzača schválilo proces neustáleho zlepšovania a monitorovania ISMS, tak aby bolo zabezpečené, že systém bude aktuálny a účinný v priebehu času.
- Alokácia zdrojov: dokument/doklad, v ktorom vedenie uchádzača sa zaviazalo zabezpečiť, že organizácia bude poskytovať potrebné ľudské, technické a finančné zdroje na podporu implementácie a údržby ISMS.

Otázka č. 17:
Uchádzač vo svojej odpovedi predložil dokument s názvom *„System manazerstva informacnej bezpecnosti v spolocnosti ANTIK Telecom s.r.o..pdf“*, zo dňa 28.03.2025, ktorý vypracoval p.Oliver Nemčik, Manažér Kybernetickej bezpečnosti, Antik Telecom s.r.o. v bode 11 Súlad uviedol tabuľku s porovnaním požiadaviek ISO/IEC 27002 a požiadavkami Zákona č. 69/2018 Z.z.:

ISO/IEC 27002 Požiadavka	Požiadavky Zákona 69/2018 Z.z SR
Politiky informačnej bezpečnosti	§ 20, písm. 3 Bezpečnostné opatrenia sa prijímajú a realizujú v rozsahu a spôsobom podľa § 32 ods. 1 písm. b) alebo osobitného predpisu, ak je vydaný, a na základe schválenej bezpečnostnej dokumentácie, ktorá musí byť aktuálna a musí zodpovedať reálnemu stavu.
Organizácia informačnej bezpečnosti	§ 20, písm. 2 a)organizácia a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti
Bezpečnosť ľudských zdrojov	§ 20, písm. 2 i) bezpečnosť a spôsobilosti ľudských zdrojov
Správa aktív	§ 20, písm. 2 c) správu aktív a riadenie kybernetických hrozieb a rizík
Kontrola prístupu	§ 20, písm. 2 j) správu identít a prístupov
Kryptografia	§ 20, písm. 2 h) kryptografické opatrenia a zásady používania kryptografie
Fyzická a environmentálna bezpečnosť	§ 20, písm. 2 o) fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení
Bezpečnosť prevádzky	§ 20, písm. 2 k)bezpečnosť pri prevádzke sietí a informačných systémov
Bezpečnosť komunikácií	§ 20, písm. 2 m) systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť
Nákup, vývoj a údržba systémov	§ 20, písm. 2 f) bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií
Vzťahy s dodávateľmi	§ 20, písm. 2 q)dodávateľský reťazec
Riadenie incidentov bezpečnosti informácií	§ 20, písm. 2 n)monitorovanie, zaznamenávanie a hlásenie udalostí
Aspekty bezpečnosti informácií pri riadení kontinuity podnikania	§ 20, písm. 2 e) riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie
Súlad	§ 20, písm. 2 g) postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti

Tabuľka č.1

Nižšie uvádzame vo forme tabuľky (Tabuľka č.2) porovnanie/analýzu oblasti/požiadavky normy ISO 27001:2013 a ich pokrytie zákonom 69/2018 Z. z.v súbehu s vyhláškou NBÚ č. 362/2018:

Oblasť / požiadavka ISO 27001:2013	Pokrytie zákonom 69/2018 Z.z. + vyhl. 362/2018 Z.z.	Komentár
4.1 Kontext organizácie	Zákon sa nezaoberá kontextom, len bezpečnostnými opatreniami	Zákon č. 69/2018 Z.z. ani vyhláška č. 362/2018 Z.z. nevyžadujú, aby organizácia formálne posudzovala svoj vonkajší a vnútorný kontext, ako to požaduje ISO 27001. Norma očakáva, že organizácia identifikuje faktory ako právne prostredie, zainteresované strany, kultúru či technologické trendy, ktoré môžu ovplyvniť jej ISMS. V rámci auditu sa takýto širší strategický rámec nevyhodnocuje.
4.2 Zainteresované strany a ich požiadavky	Nepokrýva sa	ISO 27001 požaduje, aby organizácia identifikovala všetky relevantné zainteresované strany (napr. zákazníci, partneri, regulačné orgány) a ich požiadavky na informačnú bezpečnosť. Tieto očakávania majú byť zohľadnené pri plánovaní ISMS. V rámci zákona 69/2018 Z.z. ani vyhlášky 362/2018 Z.z. sa takýto koncept nenachádza – legislatíva sa zameriava výlučne na plnenie povinností voči NBÚ a bezpečnostným opatreniam, nie na širšie vzťahy a očakávania.
4.3 Rozsah ISMS	Vymedzenie rozsahu opatrení v dokumentácii je povinné	Zákona 69/2018 Z.z. a vyhláška 362/2018 Z.z. požadujú vymedzenie rozsahu bezpečnostných opatrení (napr. ktoré systémy sú klasifikované ako základná služba), norma ISO/IEC 27001:2013 definuje rozsah ISMS ako systematické vymedzenie hraníc a aplikovateľnosti systému manažérstva informačnej bezpečnosti, vrátane prevádzok, procesov a tretích strán. Rozsah ISMS musí byť formálne zdokumentovaný a zdôvodnený. V rámci auditu podla Zákon 69/2018 Z.z. sa rozsah stanovuje z pohľadu zákona, nie z pohľadu systému riadenia, čo by znamenalo, že organizácia by túto časť musela rozšíriť a doplniť pre účely ISO certifikácie.
4.4 ISMS – systémové riadenie bezpečnosti	Nie je požadovaný kompletný ISMS ako systém	Zákon ani vyhláška nevyžadujú systematický prístup k informačnej bezpečnosti ako manažérsky systém (ISMS). ISO 27001 kladie dôraz na cyklus PDCA (Plan-Do-Check-Act), neustále zlepšovanie a dokumentovanú správu systému. Na rozdiel od toho zakon 69/2018 Z.z. a vyhláška - audit kontroluje, či sú implementované konkrétne bezpečnostné opatrenia – bez hodnotenia systému ako celku, bez väzby na interné audity, zlepšovanie alebo management review. Implementácia ISMS je tak zásadný doplnok nad rámec zákonných požiadaviek.
5.1 Leadership a záväzok vedenia	Povinné je menovať zodpovednú osobu, ale nie leadership ako ISO definuje	Audit podľa zákona 69/2018 Z.z. vyžaduje menovanie osoby zodpovednej za kybernetickú bezpečnosť (manažéra kybernetickej bezpečnosti), ISO 27001 kladie dôraz na aktívnu účasť vrcholového vedenia v ISMS. To zahŕňa preukázateľný záväzok, že vedenie definuje politiku, zabezpečuje zdroje, podporuje zlepšovanie a vedie strategické preskúmania. V rámci auditu podľa Zákona 69/2018 Z.z. sa záväzok vedenia neoveruje ako samostatná povinnosť

Oblasť / požiadavka ISO 27001:2013	Pokrytie zákonom 69/2018 Z.z. + vyhl. 362/2018 Z.z.	Komentár
5.2 Politika informačnej bezpečnosti	Výslovne požadovaná v dokumentácii (§ 3, § 4 vyhlášky)	
5.3 Roly a zodpovednosti	Menovanie MKB a ďalších rolí je povinné	
6.1.1 Zohľadnenie rizík a príležitostí	Audit rieši len hrozby a riziká, nie príležitosti	ISO 27001 vyžaduje, aby organizácia pri plánovaní ISMS zohľadnila nielen riziká, ale aj príležitosti na zlepšenie systému. Zákon 69/2018 Z.z. a vyhláška 362/2018 Z.z. sa zameriava výlučne na identifikáciu a zvládanie hrozieb, ktoré by mohli ohroziť kybernetickú bezpečnosť. Audit sa nezaoberá pozitívnymi aspektmi, ako sú možnosti zefektívnenia, inovácie alebo optimalizácie procesov.
6.1.2 Analýza rizík	Povinná súčasť dokumentácie a auditu	
6.1.3 Ošetrenie rizík + SoA (Statement of Applicability)	Bez explicitného SoA – len popis plnenia opatrení	Vyhláška 362/2018 Z.z. vyžaduje popis bezpečnostných opatrení, ale nepozná koncept prehlásenia o aplikovateľnosti (SoA), ktorý ISO norma vyžaduje ako povinný dokument. SoA podľa ISO obsahuje výber kontrol z Annex A, dôvod ich zaradenia alebo nezaradenia, stav implementácie a ich väzbu na riadenie rizík. V audite podla zákona 69/2018 Z.z. sa hodnotí, či organizácia plní povinné opatrenia, ale nie, či si tieto opatrenia zvolila na základe analýzy rizík a v rámci širšieho ISMS.
6.2 Ciele IS bezpečnosti a plán ich dosiahnutia	Zákon nepožaduje stanovovanie cieľov	ISO norma vyžaduje, aby si organizácia stanovila merateľné ciele v oblasti informačnej bezpečnosti (napr. znížiť počet incidentov, skrátiť čas reakcie) a vytvorila plány, ako ich dosiahne. Zákon 69/2018 Z.z. sa sústreďuje na minimálne opatrenia – nevyžaduje, aby organizácia určovala ciele, sledovala ich napĺňanie alebo vyhodnocovala výsledky. Ide teda o úplne rozdielny prístup: ISO kladie dôraz na výkon a zlepšovanie, zatiaľ čo Zákon 69/2018 Z.z. kontroluje len plnenie zákonného minima bez sledovania progresu.
7.1 Zdroje	Predpokladajú sa, ale nie sú výslovne auditované	
7.2 Kompetentnosť	Vyžaduje sa len pre MKB, nie systémovo	Zákon 69/2018 Z.z. vyžaduje, aby bol manažér kybernetickej bezpečnosti odborník so znalosťami a skúsenosťami, ISO norma rozširuje túto požiadavku na všetky osoby, ktoré majú vplyv na bezpečnosť ISMS – od správcov systémov až po vývojárov. Okrem toho ISO požaduje hodnotenie spôsobilosti a plány na jej zvyšovanie. Audit podla Zákona 69/2018 Z.z. sa týmto detailom nevenuje.

Oblasť / požiadavka ISO 27001:2013	Pokrytie zákonom 69/2018 Z.z. + vyhl. 362/2018 Z.z.	Komentár
7.3 Povedomie a školenia	Predpokladá sa školenie, ale bez metód povedomia	
7.4 Komunikácia (interná/externá)	Externá (s NBÚ) áno, interná nie	Legislatíva vyžaduje, aby organizácia komunikovala s NBÚ v prípade kybernetických incidentov a vymenovala kontaktnú osobu, ISO komunikáciu rozširuje a stanovuje, že organizácia musí plánovať internú a externú komunikáciu vrátane toho, čo sa komunikuje, kto, kedy a ako. Týka sa to napríklad oznamovania politiky bezpečnosti, interných porušení pravidiel alebo reakcií na otázky zákazníkov. ISO vyžaduje konzistentnú, riadenú a vopred definovanú komunikačnú stratégiu ako súčasť ISMS
7.5 Dokumentované informácie (systémové riadenie dokumentov)	Vyžaduje sa popis a vedenie bezpečnostnej dokumentácie	
8.1 Plánovanie a prevádzka opatrení	Veľmi dôsledne kontrolované (prevádzkové zabezpečenie)	
9.1 Monitorovanie, meranie, analýza a hodnotenie	Audit zisťuje účinnosť, ale nie sú povinné metriky ISMS	Audit posudzuje, či sú implementované bezpečnostné opatrenia a či existuje dokumentácia – ale nevyžaduje aktívne monitorovanie výkonnosti systému ISMS. ISO 27001 žiada nastaviť metriky a mechanizmy, ako organizácia bude pravidelne vyhodnocovať účinnosť bezpečnostných opatrení (napr. počet incidentov, čas riešenia, úroveň súladu). Tieto ukazovatele slúžia na riadenie výkonnosti a zlepšovanie systému. Bez nich organizácia nepreukáže, že ISMS skutočne funguje efektívne
9.2 Interný audit ISMS	Nevyžaduje sa interný audit – iba externý	ISO 27001 kladie dôraz na pravidelné interné audity systému ISMS s cieľom overiť jeho súlad, účinnosť a pripravenosť na certifikáciu, zákon č. 69/2018 Z.z. žiadnu takúto požiadavku neobsahuje. Vyhláška 362/2018 Z.z. predpokladá len externý audit vykonávaný NBÚ alebo certifikovaným audítorom. Organizácia teda nemusí mať zavedený mechanizmus vlastného preverovania systému, čím chýba dôležitý prvok spätného riadenia kvality ISMS.

Oblasť / požiadavka ISO 27001:2013	Pokrytie zákonom 69/2018 Z.z. + vyhl. 362/2018 Z.z.	Komentár
9.3 Preskúmanie vedením (management review)	Nie je legislatívne požadované	Preskúmanie vedením je základnou požiadavkou ISO 27001, ktorá má zabezpečiť, že vrcholový manažment pravidelne hodnotí výkonnosť ISMS a prijíma rozhodnutia o zlepšovaní. Obsahuje prvky ako vyhodnotenie cieľov, výsledkov auditov, stavu incidentov či zmien v prostredí. V zákone o kybernetickej bezpečnosti a vyhláške č. 362/2018 Z.z. sa takáto činnosť od vedenia organizácie nevyžaduje – zodpovednosť je delegovaná na MKB.
10.1 Nezhody a nápravné opatrenia	Nápravné opatrenia sa požadujú, ale procesne nie sú štandardizované	Po audite je organizácia povinná navrhnúť nápravné opatrenia k zisteným nedostatkom, zákon nevyžaduje, aby existoval formálny, dokumentovaný proces riadenia nezhôd. ISO norma definuje, že každá nezhoda musí byť zdokumentovaná, musí sa vykonať analýza príčin, prijať opatrenia a overiť ich účinnosť. Tento proces je kľúčový pre budovanie efektívneho ISMS. V legislatívnom audite sa predpokladá reaktívne odstránenie zistení, ale nie systematické zlepšovanie procesu.
10.2 Neustále zlepšovanie	Nie je požadované – cieľ je "súlad", nie zlepšovanie	
Všetky zákonné požiadavky ako záväzné GDPR	Zákon sa sústreďuje na technické a organizačné opatrenia na ochranu informačných systémov, prevenciu a riadenie incidentov, kategorizáciu systémov, klasifikáciu aktív a dokumentáciu opatrení podľa vyhlášky.	V kapitole 6.1.3 (ošetrenie rizík) a v prílohe A.18.1.1 (Identification of applicable legislation) je výslovne uvedené, že organizácia musí identifikovať všetky zákonné požiadavky, ktoré sa na ňu vzťahujú – teda aj GDPR, ak spracúva osobné údaje občanov EÚ.

Tabuľka č.2

Z uvedeného porovnania (uvedeného v Tabuľke č.2) vyplýva, že zákon 69/2018 Z.z. nepokrýva oblasti/požiadavky ISO 27001:2013 v bodoch 4.2, 4.4, 6.1.1, 9.2, 9.3, 10.2 a taktiež nepreukazuje legislatívny súlad v zmysle požiadavky bodu A.18.1.1 normy ISO 27001 a tiež nezahŕňa ani hodnotenie súladu s nariadením GDPR.

V súlade s požiadavkou **bodu A.18.1.1** normy **ISO/IEC 27001:2013** je organizácia **povinná identifikovať a preukázateľne evidovať všetky legislatívne, regulačné a zmluvné požiadavky**, ktoré sa na ňu vzťahujú. Táto požiadavka zahŕňa **komplexný legislatívny rámec krajiny, kde organizácia pôsobí**, a to vrátane **nariadenia GDPR (2016/679)**, ak organizácia spracúva osobné údaje občanov EÚ.

Naopak, **audit vykonávaný v súlade so zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti**, a jeho vykonávacou **vyhláškou č. 362/2018 Z. z.**, má **obmedzený rozsah**. Jeho cieľom je **overiť súladnosť organizácie s povinnosťami vyplývajúcimi výlučne z tohto zákona a súvisiacich podzákonných predpisov**, predovšetkým:

- plnenie bezpečnostných opatrení,

- vypracovanie bezpečnostnej dokumentácie,
- hodnotenie rizík podľa NBU metodiky,
- oznamovanie kybernetických bezpečnostných incidentov atď.

Audit podľa zákona o kybernetickej bezpečnosti teda:

- neoveruje celkový súlad organizácie so všetkými právnymi predpismi SR (napr. zákon o ochrane osobných údajov),
- a rovnako nezahŕňa ani hodnotenie súladu s nariadením GDPR, pokiaľ to nie je explicitne súčasťou iného právneho alebo zmluvného rámca.

ISO/IEC 27001:2013 kladie dôraz na identifikáciu a evidenciu všetkých aplikovateľných legislatívnych požiadaviek (A.18.1.1), čo zahŕňa **GDPR aj iné sektorové zákony**. Naproti tomu, **audit podľa zákona č. 69/2018 Z. z. je špecializovaný audit**, ktorý sa **výhradne zameriava na splnenie povinností vyplývajúcich z kybernetickej legislatívy**, a **nezastupuje širší audit právneho súladu organizácie**.

Na základe uvedeného, verejný obstarávateľ žiada vysvetliť:

A. vyššie uvedenú nezrovnalosť vyplývajúcu z vyššie uvedeného porovnania a to, že zákon 69/2018 Z.z. nepokrýva oblasti/požiadavky ISO 27001:2013 v bodoch 4.2, 4.4, 6.1.1, 9.2, 9.3, 10.2 a č. A.18.1.1 (preukázanie legislatívneho súladu) a nezahrnutie hodnotenie súladu s nariadením GDPR.

B. Na základe predloženej dokumentácie vyplýva, že uchádzač sa pri preukazovaní ekvivalentnosti auditu vykonávaného podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti s certifikáciou podľa normy ISO/IEC 27001:2013 odvoláva na tzv. mapovanie požiadaviek medzi týmito dvoma rámcami (tabuľka č. 1).
   V tejto súvislosti žiadame uchádzača o vysvetlenie, prečo pri tomto mapovaní neporovnával tzv. „základné oblasti a požiadavky normy ISO/IEC 27001:2013“ (kapitoly 4 až 10 normy), ktoré definujú základný rámec riadenia ISMS – napr. kontext organizácie, riadenie rizík, plánovanie opatrení, monitorovanie výkonnosti či zlepšovanie systému –, ale zameral sa výlučne na porovnanie s tzv. doménovým členením prílohy A (Annex A: A.5 až A.18).
   Z odborného hľadiska však príloha A predstavuje iba referenčný súbor bezpečnostných opatrení („reference control objectives and controls“), ktoré nepredstavujú úplný rámec systému riadenia informačnej bezpečnosti (ISMS), ale slúžia ako podporný nástroj na mitigáciu identifikovaných rizík.
   Časti 4 až 10 normy ISO/IEC 27001:2013 – tzv. hlavná časť normy – sú pritom normatívne, teda záväzné pre účely certifikácie, a definujú požiadavky na zavedenie, prevádzku, monitorovanie, preskúmanie a neustále zlepšovanie ISMS.
   Táto časť:
   - nešpecifikuje konkrétne bezpečnostné opatrenia, ale
   - vyžaduje identifikáciu rizík (čl. 6.1),
   - určenie opatrení na ich ošetrenie (čl. 6.1.3),
   - a formálne preukázanie výberu opatrení v podobe Vyhlásenia o aplikovateľnosti (Statement of Applicability – SoA).

   Z vyššie uvedeného vyplýva, že časť 4–10 a príloha A normy sú síce komplementárne, avšak štruktúrne rozdielne a s odlišným účelom.
   Preto žiadame objasniť, z akého dôvodu považuje uchádzač porovnanie výlučne na úrovni opatrení prílohy A za postačujúce pre preukazovanie ekvivalentnosti s certifikáciou podľa ISO/IEC 27001, a zároveň akým spôsobom boli (ak vôbec) v jeho posúdení zohľadnené požiadavky hlavnej normatívnej časti (kap. 4–10), ktoré nie sú súčasťou vyhlášky č. 362/2018 Z. z. ani zákona č. 69/2018 Z. z.

C. Žiadame vysvetliť, prečo uchádzač v porovnaní porovnal požiadavky normy ISO/IEC27002 miesto IS/IEC/27001:2013, ktoré boli predmetom žiadosti o vysvetlenie.

V záujme preukázania súladnosti s ISO/IEC 27001 **žiadame uchádzača, aby v rámci odpovedí na otázky č. 1 až 12** preukázal skutočnosť, že odpovede na jednotlivé otázky sú obsahom príslušných kapitol zavedeného systému ISMS.

Verejný obstarávateľ zároveň upozornil, že v prípade nedoručenia vysvetlenia/doplnenia v stanovenej lehote verejný obstarávateľ v súlade s § 40 ods. 6 písm. h) ZVO pristúpi k vylúčeniu ponuky z predmetnej verejnej súťaže.

Prílohou žiadosti o vysvetlenie bolo aj 114 kontrolných opatrení podľa ISOIEC 27001-2013 (Annex A)

Uchádzač č. 5 Antik Telekom, s.r.o. dňa 11.06.2025 prostredníctvom systému na elektronickú komunikáciu IS Josephine doručil Žiadosť o predĺženie lehoty na predloženie vysvetlenia č. 2 podľa § 40 ods. 4 ZVO, v ktorej uvádza:

„Uchádzač ANTIK Telecom s.r.o., Čárskeho 10, 040 01 Košice, IČO: 36 191 400, predložil v rámci nadlimitnej zákazky: Digitálna infraštruktúra škôl - vytvorenie riešenia na školách a prevádzka komplexných telekomunikačných služieb LAN/WLAN/WAN Košický kraj, číslo uverejnenia oznámenia v Úradnom vestníku EÚ: 800967-202, číslo vydania série S úradného vestníka: 253/2024 zo dňa 31/12/2024, zverejnená v národnom Vestníku verejného obstarávania č. 1/2025 pod číslom 12 – MSS, dátum zverejnenia 02.01.2025 vyhlásená verejným obstarávateľom: Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, Černyševského 50, 851 01 Bratislava, IČO: 00 164 381 cenovú ponuku dňa 14.02.2025. Na základe žiadosti o predloženie dokladov nahradených JED formulárom predložil uchádzač dňa 27.02.2025 doklady na preukázanie splnenia podmienok účasti, na čo verejný obstarávateľ zaslal uchádzačovi dňa 21.03.2025 žiadosť o vysvetlenie podľa § 40 ods. 4 ZVO. Uchádzač predložil vysvetlenie vo verejným obstarávateľom stanovenej lehote, t.j. do 31.03.2025 do 11:00 hod.

Verejný obstarávateľ dňa 06.06.2025 zaslal uchádzačovi žiadosť o vysvetlenie č. 2 podľa § 40 ods. 4 ZVO v rozsahu sedemnástich (17) otázok s viacerými podotázkami rozpísaných na 16 stranách žiadosti o vysvetlenie po vyše troch mesiacoch vyhodnocovania predložených dokumentov preukazujúcich splnenie podmienky účasti a vysvetlenia týchto dokumentov, pričom uchádzačovi poskytol lehotu na vysvetlenie 5 pracovných dní.

Vzhľadom na uvedené žiada týmto uchádzač o predĺženie lehoty na vysvetlenie/doplnenie predložených dokumentov z dôvodu rozsahu požadovaného vysvetlenia, obsahovo a časovo náročného spracovania požadovaného porovnania dokumentov, pričom je potrebné na spracovanie vysvetlenia spolupracovať s externým audítorom, a to v rozsahu najmenej o 30 kalendárnych dní.“

Verejný obstarávateľ dňa 12.06.2025 prostredníctvom systému na elektronickú komunikáciu IS Josephine zaslal odpoveď na žiadosť o predĺženie lehoty na predloženie vysvetlenia, v ktorej čiastočne vyhovel žiadosti a lehotu na predloženie vysvetlenia č. 2 predĺžil do 20.06.2025 do 11:00 hod.

V rámci odpovedi na žiadosť o predĺženie lehoty na predloženie vysvetlenia k žiadosti o vysvetlenie č. 2 o 30 dní verejný obstarávateľ uviedol:

„Verejný obstarávateľ Vás, ako uchádzača ktorý predložil ponuku v rámci nadlimitnej zákazky: Digitálna infraštruktúra škôl - vytvorenie riešenia na školách a prevádzka komplexných telekomunikačných služieb LAN/WLAN/WAN Košický kraj, číslo uverejnenia oznámenia v Úradnom vestníku EÚ: 800967-202, číslo vydania série S úradného vestníka: 253/2024 zo dňa 31/12/2024, zverejnená v národnom Vestníku verejného obstarávania č. 1/2025 pod číslom 12 – MSS, dátum zverejnenia 02.01.2025 vyhlásenej verejným

obstarávateľom: Ministerstvo školstva, výskumu, vývoja a mládeže Slovenskej republiky, Černyševského 50, 851 01 Bratislava, IČO: 00 164 381 požiadal o doručenie vysvetlenia v zmysle § 40 ods. 4 ZVO.

Verejný obstarávateľ Vám prostredníctvom systému na elektronickú komunikáciu IS Josephine dňa 06.06.2025 zaslal žiadosť o vysvetlenie č. 2 podľa § 40 ods. 4 ZVO s lehotou doručenia vysvetlenia do 16.06.2025 do 14:00 hod.

Dňa 11.06.2025 od Vás verejný obstarávateľ prostredníctvom IS Josephine obdržal žiadosť o predĺženie lehoty na predloženie vysvetlenia, v ktorej žiadate o predĺženie lehoty na doručenia vysvetlenia v rozsahu o 30 dní.

Svoju žiadosť odôvodňujete rozsahom požadovaného vysvetlenia, obsahovo a časovo náročného spracovania požadovaného porovnania dokumentov, pričom je potrebné na spracovanie vysvetlenia spolupracovať s externým audítorom, a to v rozsahu najmenej o 30 kalendárnych dní.

Na základe Vašej žiadosti Vám verejný obstarávateľ oznamuje, že vyhovuje čiastočne a oznamuje novú lehotu na predloženie vysvetlenia k žiadosti o vysvetlenie č. 2 na 20.06.2025 do 11:00 hod.

Verejný obstarávateľ považuje takto stanovenú celkovú lehotu v rozsahu 13 dní za dostatočnú a primeranú na spracovanie a predloženie odpovedí a dôkazov.

V tejto súvislosti ďalej uvádzame, že za prípravu ponuky zodpovedá uchádzač, pričom ten ju môže meniť len v lehote na predkladanie ponúk. Dodatočné rozšírenie ponuky (predloženie rozšíreného počtu dokumentov/dokladov preukazujúcich splnenie podmienok účasti oproti dokumentom uvedeným v ponuke) po uplynutí lehoty na predkladanie ponúk nie je vzhľadom na dodržanie predovšetkým princípov rovnakého zaobchádzania a nediskriminácie uchádzačov možné. Inštitút vysvetľovania ponuky neslúži na to, aby poskytoval dodatočný časový priestor pre vyhotovenie, resp. úpravu ponuky, t. j. na zabezpečenie dodatočných kapacít, predkladanie dodatočných dokladov a pod. Určité výnimky voči uvedenému, kedy je možné doplňať/meniť ponuku aj podstatným spôsobom predstavujú nástroje samoočisťovacieho mechanizmu alebo nahradenia tretích osôb či subdodávateľov. Na to však musia byť splnené zákonom predpokladané podmienky. Z uvedeného vyplýva, že inštitút vysvetľovania ponuky nemá slúžiť na to, aby poskytoval dodatočný časový priestor pre vyhotovenie, resp. úpravu ponuky, t. j. na zabezpečenie dodatočných kapacít, predkladanie dodatočných dokladov a podobne.

Zároveň dávame do pozornosti, že <u>verejný obstarávateľ v rámci vysvetlenia nežiadal predloženie novovytvorených dokumentov, požadoval len predloženie dôkazov o zavedení / implementácie postupov, čiže požadoval predloženie už existujúcich dokladov/dokumentov preukazujúcich zavedenie jednotlivých podkategórií normy</u> ISO /IEC 27001:2013 napríklad formou riadiacich aktov, či už napríklad predloženie príslušnej prijatej smernice, príkazu vedenia spoločnosti a podobne.“

Verejný obstarávateľ zároveň uchádzača č. 5 Antik Telekom, s.r.o. upozornil, že v prípade nedoručenia vysvetlenia/doplnenia v stanovenej lehote verejný obstarávateľ v súlade s § 40 ods. 6 písm. h) ZVO pristúpi k vylúčeniu ponuky z predmetnej verejnej súťaže.

Uchádzač č. 5 Antil Telekom, s.r.o. v stanovenej lehote nedoručil vysvetlenie.

Komisia v súlade s § 40 ods. 6 písm. h) ZVO pristúpila k vylúčeniu ponuky z verejnej súťaže z dôvodu nepredloženia po písomnej žiadosti podľa odseku 4 vysvetlenie alebo doplnenie predložených dokladov v určenej lehote.

15. Zoznam záujemcov/uchádzačov, ktorí budú vyzvaní na vysvetlenie/doplnenie podľa § 40 ods. 4 ZVO: viď bod 14
16. Zoznam vylúčených uchádzačov/záujemcov s uvedením dôvodu ich vylúčenia: uchádzač č. 5 Antik Telekom, s.r.o., Čárskeho 10, 04 001 Košice, IČO: 36191400 v súlade s § 40 ods. 6 písm. h) ZVO z dôvodu nepredloženia po písomnej žiadosti podľa odseku 4 vysvetlenie alebo doplnenie predložených dokladov v určenej lehote

17. Zoznam vybratých záujemcov, resp. záujemcov, ktorí budú vyzvaní na predloženie ponuky a dôvody ich výberu v užšej súťaži a v rokovacom konaní so zverejnením: Neaplikuje sa
18. Zoznam záujemcov, ktorí nebudú vyzvaní na predloženie ponuky alebo na rokovanie s uvedením dôvodu[1]: neaplikuje sa

Členovia komisie na vyhodnotenie ponúk vyhlasujú, že táto zápisnica zodpovedá skutočnosti, čo potvrdzujú svojim podpisom.

P. č.	Meno	Funkcia	Podpis
1.	Ing. Alexander Šproch	predseda komisie s právom vyhodnocovať ponuky a komunikovať v mene zadávateľa	
2.	Ing. Ján Jasenák	člen komisie s právom vyhodnocovať ponuky	
3.	Ing. Ivan Šiagi	člen komisie s právom vyhodnocovať ponuky	
4.	Ing. Štefan Mačica	člen komisie s právom vyhodnocovať ponuky	
5.	Ing. Vladimír Pokojný	člen komisie bez práva vyhodnocovať ponuky, administrátor zákazky	
6.	Mgr. Schlosserová Silvia	členka komisie bez práva vyhodnocovať ponuky, administrátor zákazky	

V Bratislave, dňa 01.07.2025

Zapísal: Ing. Vladimír Pokojný

člen komisie

Prílohy:

- DigiEDU NR Príloha č. 1a zápisnice z vyhodnotenia splnenia podmienok účasti SLOVANET
- DigiEDU NR Príloha č. 1b zápisnice z vyhodnotenia splnenia podmienok účasti SWAN
- DigiEDU NR Príloha č. 1c zápisnice z vyhodnotenia splnenia podmienok účasti SLOVAK TELEKOM
- DigiEDU NR Príloha č. 1d zápisnice z vyhodnotenia splnenia podmienok účasti O2 Business Services
- DigiEDU NR Príloha č. 1e zápisnice z vyhodnotenia splnenia podmienok účasti ANTIK
- Výpisy z Obchodného registra SR
- Výpisy zo Zoznamu hospodárskych subjektov vedenom na ÚVO
- Výpisy zo Zoznamu hospodárskych subjektov zo zákazom účasti

Upozornenie: V zápisnici je potrebné uviesť všetky situácie, ktorými sa prijímateľ zaoberal a vysvetliť, ako sa s nimi vysporiadal, napr. uviesť zdôvodnenie, prečo požiadal o vysvetlenie, v prípade neakceptovania niektorého z dokumentov uviesť, prečo nepožiadal záujemcu/uchádzača o vysvetlenie a pod.

[1] Použije sa v prípade užšej súťaže, alebo rokovacieho konania so zverejnením.