UOHSX00CY69D

ÚŘAD PRO OCHRANU HOSPODÁŘSKÉ SOUTĚŽE

ROZHODNUTÍ

Č. j.: ÚOHS-S0358/2019/VZ-01269/2020/512/KMo Brno: 13. ledna 2020

Úřad pro ochranu hospodářské soutěže příslušný podle § 248 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, ve správním řízení zahájeném dne 23. 9. 2019 na návrh z téhož dne, jehož účastníky jsou

- zadavatel – Metropolnet, a.s., IČO 25439022, se sídlem Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem,
- navrhovatel – Huawei Technologies (Czech) s.r.o., IČO 27367061, se sídlem Jihlavská 1558/21, Michle, 140 00 Praha 4,

ve věci přezkoumání úkonů zadavatele učiněných při zadávání veřejné zakázky „Obnova páteřní a přístupové infrastruktury“ v otevřeném řízení, jehož oznámení bylo odesláno k uveřejnění dne 23. 7. 2019 a uveřejněno ve Věstníku veřejných zakázek dne 26. 7. 2019 pod ev. č. zakázky Z2019-025302, a v Úředním věstníku Evropské unie uveřejněno dne 26. 7. 2019 pod ev. č. 2019/S 143-351497,

rozhodl takto:

I.

Zadavatel – Metropolnet, a.s., IČO 25439022, se sídlem Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem – **stanovil zadávací podmínky v zadávacím řízení** na veřejnou zakázku „Obnova páteřní a přístupové infrastruktury“ zadávanou v otevřeném řízení, jehož oznámení bylo odesláno k uveřejnění dne 23. 7. 2019 a uveřejněno ve Věstníku veřejných zakázek dne 26. 7. 2019 pod ev. č. zakázky Z2019-025302, a v Úředním věstníku Evropské unie uveřejněno dne 26. 7. 2019 pod ev. č. 2019/S 143-351497, **v rozporu s ustanovením § 36 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů ve spojení se**

zásadou zákazu diskriminace zakotvenou v ustanovení § 6 odst. 2 citovaného zákona tím, že stanovil zadávací podmínky tak, že vytvářely bezdůvodné překážky hospodářské soutěže, když v článku 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace mj. stanovil, že vylučuje technické a programové prostředky společností Huawei Technologies Co., Ltd., Šen-Čen, Čínská lidová republika a ZTE Corporation, Šen-Čen, Čínská lidová republika, včetně jejich dceřiných společností, z předmětného zadávacího řízení, a to s odvoláním na „Varování č. j. 3012/2018-NÚKIB-E/110“ ze dne 17. 12. 2018 a „Metodiku k varování ze dne 17. prosince 2018“ ze dne 4. 1. 2019 vydanými Národním úřadem pro kybernetickou a informační bezpečnost, ačkoliv neexistovaly relevantní důvody na straně citovaného zadavatele pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu výše uvedené technické a programové prostředky, a citovaný zadavatel tak nedodržel zásadu zákazu diskriminace ve vztahu k navrhovateli – Huawei Technologies (Czech) s.r.o., IČO 27367061, se sídlem Jihlavská 1558/21, Michle, 140 00 Praha 4.

II.

Jako opatření k nápravě nezákonného postupu zadavatele – Metropolnet, a.s., IČO 25439022, se sídlem Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem – uvedeného ve výroku I. tohoto rozhodnutí Úřad pro ochranu hospodářské soutěže podle ustanovení § 263 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, **ruší zadávací řízení na veřejnou zakázku** „Obnova páteřní a přístupové infrastruktury“ zadávanou v otevřeném řízení, jehož oznámení bylo odesláno k uveřejnění dne 23. 7. 2019 a uveřejněno ve Věstníku veřejných zakázek dne 26. 7. 2019 pod ev. č. zakázky Z2019-025302, a v Úředním věstníku Evropské unie uveřejněno dne 26. 7. 2019 pod ev. č. 2019/S 143-351497.

III.

Zadavateli – Metropolnet, a.s., IČO 25439022, se sídlem Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem – **se** podle ustanovení § 263 odst. 8 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, až do pravomocného skončení správního řízení vedeného Úřadem pro ochranu hospodářské soutěže pod sp. zn. S0358/2019/VZ ve věci návrhu navrhovatele – Huawei Technologies (Czech) s.r.o., IČO 27367061, se sídlem Jihlavská 1558/21, Michle, 140 00 Praha 4 – ze dne 23. 9. 2019 na zahájení správního řízení o přezkoumání úkonů zadavatele **ukládá zákaz uzavřít smlouvu v zadávacím řízení** na veřejnou zakázku „Obnova páteřní a přístupové infrastruktury“ zadávanou v otevřeném řízení, jehož oznámení bylo odesláno k uveřejnění dne 23. 7. 2019 a uveřejněno ve Věstníku veřejných zakázek dne 26. 7. 2019 pod ev. č. zakázky Z2019-025302, a v Úředním věstníku Evropské unie uveřejněno dne 26. 7. 2019 pod ev. č. 2019/S 143-351497.

IV.

Podle ustanovení § 266 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, v návaznosti na § 1 vyhlášky č. 170/2016 Sb., o stanovení paušální částky nákladů řízení o přezkoumání úkonů zadavatele při zadávání veřejných zakázek, se zadavateli – Metropolnet, a.s., IČO 25439022, se sídlem Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem – ukládá povinnost

uhradit náklady řízení ve výši 30 000,- Kč (třicet tisíc korun českých)

Náklady řízení jsou splatné do dvou měsíců od nabytí právní moci tohoto rozhodnutí.

ODŮVODNĚNÍ

I. ZADÁVACÍ ŘÍZENÍ

1. Zadavatel – Metropolnet, a.s., IČO 25439022, se sídlem Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem (dále jen „zadavatel“) – zahájil podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon“), zadávací řízení na veřejnou zakázku „Obnova páteřní a přístupové infrastruktury“ zadávanou v otevřeném řízení, jehož oznámení bylo odesláno k uveřejnění dne 23. 7. 2019 a uveřejněno ve Věstníku veřejných zakázek dne 26. 7. 2019 pod ev. č. zakázky Z2019-025302, a v Úředním věstníku Evropské unie uveřejněno dne 26. 7. 2019 pod ev. č. 2019/S 143-351497 (dále jen „veřejná zakázka“).

2. V bodu 5. „VYMEZENÍ PŘEDMĚTU VEŘEJNÉ ZAKÁZKY“ odst. 5.2. „Specifikace předmětu veřejné zakázky“ zadávací dokumentace ze dne 23. 7. 2019 (dále jen „zadávací dokumentace“) je předmět veřejné zakázky vymezen následovně:

   »Řešení požadované v rámci VZ bude nahrazovat zastaralé přepínače doposud používané v síti Metropolnet a.s. a po jeho celkové implementaci do sítě Metropolnet a.s. vytvoří komplexní, bezpečnostní a plně managementovatelný systém, integrovaný s dalšími částmi sítě Metropolnet a.s., včetně těch, které nejsou součástí této veřejné zakázky.

   Řešení komunikační a bezpečnostní infrastruktury přepínačů lze v souvislosti s jeho postupným nasazením do sítě Metropolnet a.s. rozdělit v tomto VŘ na celkem čtyři části řešení:

   1. *CORE přepínače pro zajištění CORE části sítě – je požadován jeden CORE přepínač.*
   2. *ACCESS/AGREGAČNÍ přepínače pro zajištění klíčových user ACCESS části sítě.*
   3. *Systém pro řízení přístupu k Datovým zdrojům sítě – Bezpečnostní funkcionalita sítě pro celkem 2 000 uživatelů.*
   4. *Nástroj pro řízení – management sítě, pro v této VZ dodávaný HW a SW.*

   Podrobná specifikace předmětu plnění je uvedena v příloze č. 2: „Kupní smlouva a smlouva o poskytnutí licence a rámcová smlouva na poskytování podpory“ a v Příloze č. 6: „Požadavky na Core a Access přepínače“. Specifikace uvedená v těchto přílohách je pro realizaci této veřejné zakázky v uvedeném rozsahu závazná.«

3. Podle bodu 4. „PŘEDPOKLÁDANÁ HODNOTA VEŘEJNÉ ZAKÁZKY“ zadávací dokumentace činí předpokládaná hodnota veřejné zakázky 19 500 000,- Kč bez DPH.

4. Dne 27. 8. 2019 byly zadavateli doručeny navrhovatelem – Huawei Technologies (Czech) s.r.o., IČO 27367061, se sídlem Jihlavská 1558/21, Michle, 140 00 Praha 4 (dále jen „navrhovatel“) – námitky ze dne 26. 8. 2019 směřující proti zadávacím podmínkám předmětné veřejné zakázky (dále jen „námitky“).

5. Námitky navrhovatele zadavatel rozhodnutím ze dne 12. 9. 2019 (dále jen „rozhodnutí o námitkách“), které bylo navrhovateli doručeno dne 12. 9. 2019, odmítl.

6. Vzhledem k tomu, že navrhovatel nesouhlasil s vyřízením svých námitek zadavatelem a má za to, že zadavatel postupoval v zadávacím řízení nezákonně, podal dne 23. 9. 2019 k Úřadu

pro ochranu hospodářské soutěže (dále jen „Úřad“) „Návrh na přezkoumání úkonů zadavatele“ ze dne 23. 9. 2019 (dále jen „návrh“).

Obsah návrhu ze dne 23. 9. 2019

7. Návrh navrhovatele směřuje proti zadávacím podmínkám veřejné zakázky a navrhovatel je přesvědčen, že zadávací podmínky jsou zadavatelem stanoveny v rozporu se zákonem, a to v rozporu s ustanovením § 36 odst. 1 zákona, v rozporu se ZKB a v rozporu s ustanovením § 6 zákona.

8. Navrhovatel ve svém návrhu v prvé řadě rekapituluje jím podané námitky a rozhodnutí o námitkách včetně skutečností pro „Oprávněnost podání návrhu na přezkoumání úkonů Zadavatele“, k čemuž navrhovatel uvádí následující skutečnosti.

9. Navrhovatel uvádí, že námitky směřovaly proti stanovení zadávací podmínky uvedené v odst. 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace, kde zadavatel mj. stanovil, že v souladu s vydaným varováním NÚKIB a metodiky NÚKIB *„provedl analýzu rizik související s plánovaným zadávacím řízením na dodávku – obnovu páteřní a přístupové infrastruktury.“*, přičemž zadavatel identifikoval rizika spojená s použitím technických a programových prostředků dotčených společností *„jako neakceptovatelná, a tedy v souladu se svými interními postupy jako nepřípustná. (…) Z důvodu obligatorně stanovené míry hrozby při využití technických a programových prostředků uvedené ve varování NÚKIB a související metodice tedy snížení rizika spojeného s používáním technických a programových prostředků dotčených společností nelze dosáhnout jinak než vyloučením technických a programových prostředků těchto společností z používání v informačních a komunikačních systémech zadavatele, a tím i jejich vyloučením z tohoto zadávacího řízení. (…) není možné technické a programové prostředky výše uvedených společností v nabídkách účastníků (včetně jejich poddodavatelů) akceptovat.“*. Navrhovatel je přesvědčen, že citovaná zadávací podmínka je stanovena v rozporu se zákonem, konkrétně v rozporu s ustanovením § 36 odst. 1 zákona, neboť určitým dodavatelům bezdůvodně zaručuje konkurenční výhodu, resp. vytváří bezdůvodné překážky hospodářské soutěže, neboť dle navrhovatele:

   (i) vybočuje z mezí opatření nezbytně nutných k plnění povinností dle ZKB, čímž v rozporu s § 4 odst. 4 ZKB a § 36 odst. 1 zákona dochází k nedůvodnému (excesivnímu) omezení hospodářské soutěže,

   (ii) je stanovena – v rozporu se ZKB – toliko na základě analýzy rizik namísto komplexního hodnocení rizik, tj. při její formulaci nebyly (v rozporu se ZKB) zohledněny kroky v rámci hodnocení rizik navazující na analýzu rizik, zejména aktualizace plánu zvládání rizik či uvážení úrovně akceptovatelného zbytkového rizika,

   (iii) je stanovena v rozporu se zásadou transparentnosti a přiměřenosti dle § 6 odst. 1 zákona,

   (iv) je stanovena v rozporu se zásadou zákazu diskriminace dle § 6 odst. 2 zákona.

10. Navrhovatel je toho názoru, že důsledkem stanovení výše uvedené zadávací podmínky *„je explicitní, předchozí vyloučení všech technických nebo programových výrobků Navrhovatele a dalších společností patřících do skupiny Navrhovatele, rovněž jako distributorů a prodejců (…), čímž byla de facto vyloučena účast Navrhovatele na veřejné zakázce (…).“*.

11. Navrhovatel ve svém návrhu dále popisuje důvody, pro které zadavatel jeho námitky odmítl.

12. Navrhovatel dále konstatuje, že jak již výše uvedl *„spatřuje porušení právních předpisů ve stanovení Zadávací podmínky uvedené v čl. 5.3. zadávací dokumentace“*, k čemuž navrhovatel uvádí následující skutečnosti.

K omezení hospodářské soutěže nad míru nezbytně potřebnou k plnění povinností dle ZKB

13. Navrhovatel ve svém návrhu uvádí, že nepopírá skutečnost, že zadavatel je vázán povinnostmi stanovenými v ZKB a nutností zohledňovat při řízení kybernetických bezpečnostních rizik souvisejících s provozováním či správou části kritické informační infrastruktury varování NÚKIB, což dle navrhovatele s sebou *„může nést nutnost stanovit pro výběr významných dodavatelů takové podmínky, které do jisté míry omezují volnou soutěž na relevantním trhu (…)“*, nicméně je přesvědčen, že se vždy musí jednat jen o takové omezení, *„které je vzhledem k okolnostem nezbytně nutné k dosažení účelu sledovaného ZKB, jak akcentuje i samotné ustanovení § 4 odst. 4 ZKB (…)“*, což podle navrhovatele není nezbytné k tomu, aby se zadavatel s varováním NÚKIB vypořádal *„plošným zákazem veškerých (byť sebemenších a z pohledu celkového řešení relativně nevýznamných) produktů (technických a programových prostředků) konkrétního výrobce, bez zohlednění jejich povahy, funkce, způsobu začlenění a významu v celkovém technickém řešení.“*.

14. V této souvislosti navrhovatel zdůrazňuje, že *„není na místě, aby Zadavatel jen na základě analýzy rizik (byť s ohledem na Varování NÚKIB indikoval vysokou míru rizika u produktů Huawei a ZTE) zcela vylučoval veškerá technická či programová řešení Huawei a ZTE (bez zohlednění jejich povahy, funkce, způsobu začlenění a významu v celkovém technickém řešení), neboť rizika plynoucí z použití takových řešení nepochybně mohou být eliminována přijetím odpovídajících (dodatečných) technických opatření, která může být dodavatel zavázán na své náklady, resp. v rámci plnění veřejné zakázky, provést (např. redundance, ochrana skrze produkty třetích osob apod.).“*, přičemž dále poukazuje na skutečnost, že i sám NÚKIB v čl. 2.2 „Co představuje institut varování“ metodiky NÚKIB mj. uvádí, že *„[v]arování tedy neznamená bezpodmínečný zákaz používání daných technických a programových prostředků.“*, přičemž, jak dále NÚKIB v metodice uvádí, samotné označení technických a programových prostředků určité společnosti za hrozbu znamená, *„že je nutné tuto hrozbu zvážit a rozhodnout o výši rizika, které z používání zmíněných technických nebo programových prostředků pro konkrétní prostředí konkrétní organizace plyne.“*.

15. Navrhovatel dále upozorňuje, že zadavatel, jako osoba povinná dle ZKB musí při volbě opatření ke snížení rizik případně identifikovaných v analýze rizik postupovat tak, aby opatření přijatá k plnění povinností dle ZKB a Vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „VKB“ či „vyhláška o kybernetické bezpečnosti“), *„co nejméně omezovala hospodářskou soutěž (srov. § 4 odst. 4 ZKB).“*.

16. Navrhovatel dále zdůrazňuje, že zadavatel *„zjevně vůbec neprovedl kroky, které musí následovat v rámci hodnocení rizik ve smyslu VKB po provedení analýzy rizik, tj. vůbec se nepokusil vymezit a zvážit vhodná opatření ke snížení identifikovaných rizik na úroveň*

akceptovaného zbytkového rizika, a to tak, aby s tím související omezení hospodářské soutěže bylo co nejmenší.“.

17. Navrhovatel ve svém návrhu dále poznamenává, že z jeho pohledu je nedůvodné *„vyloučení technických a programových prostředků společnosti Huawei i ve vztahu k těm technickým a programovým prostředkům, ve vztahu k nimž nemohly být – z povahy poptávaného plnění a konkrétního technického či programového prostředku Huawei – identifikovány žádné zranitelnosti, kterých by mohly využít hrozby, před kterými varoval NÚKIB (pozn. NÚKIB varuje pouze před určitými hrozbami, nikoli před zranitelnostmi Systému; z povahy věci přitom tam, kde není zranitelnost Systému, nemůže být ani hrozba, neboť hrozba využívá právě zranitelnosti Systému).“* a podle navrhovatele bez takové zranitelnosti *„nemůže existovat hrozba ani dopad a tím pádem ani riziko.“*.

18. Navrhovatel pak v této souvislosti uzavírá, že takovýto postup zadavatele je v rozporu se zákonem, *„když Zadavatel do zadávacích podmínek implementoval zcela excesivní opatření k plnění povinností dle ZKB, aniž by provedl úplné hodnocení rizik dle ZKB ve spojení s VKB, zejména aniž by náležitě zvážil možná opatření ke snížení rizik identifikovaných v analýze rizik, která by méně omezovala hospodářskou soutěž.“*.

K nezákonnosti stanovení předmětné zadávací podmínky bez provedení komplexního hodnocení rizik dle ZKB, resp. VKB

19. Navrhovatel ve svém návrhu uvádí, že zadavatel v rozhodnutí o námitkách uvedl, *„že předmětem námitek může být pouze polemika s obsahem zadávací dokumentace, resp. zadávacími podmínkami, nikoliv však proces, kterým Zadavatel k obsahu zadávacích podmínek dospěl, když postup tvorby zadávacích podmínek není pro jejich zákonnost rozhodný.“*, přičemž navrhovatel dále upozorňuje, že v souladu s ustanovením § 8 odst. 2 písm. a) VKB v rámci zadávacího řízení a před uzavřením smlouvy je zadavatel povinen *„provést hodnocení rizik souvisejících s plněním předmětu výběrového (zadávacího) řízení, a to přiměřeně podle přílohy č. 2 VKB“* a dále pak navrhovatel uvádí, že v souladu s ustanovením § 2 písm. d) VKB se hodnocení rizik sestává z *„(i) identifikace rizik, (ii) analýzy rizik a (iii) vyhodnocení rizik.“*, přičemž dle navrhovatele je analýza rizik *»pouze dílčí částí procesu hodnocení rizik, sloužící „toliko“ ke zjištění a stanovení úrovně rizika.«*

K rozporu se zásadou transparentnosti ve smyslu § 6 zákona

20. Navrhovatel v návrhu uvádí, že je toho názoru, že aby zadavatel neporušil zásadu transparentnosti zakotvenou v ustanovení § 6 odst. 1 zákona, musí zadavatel v zadávací dokumentaci jasně a srozumitelně popsat *„minimálně:*

- *jaká rizika byla ve vztahu k potenciálnímu využití technických a programových prostředků Huawei a ZTE identifikována; nestačí přitom pouze poukázat na hrozby dle Varování NÚKIB (…);*
- *z jakých konkrétních důvodů bylo ke snížení identifikovaných rizik zvoleno právě opatření v podobě vyloučení veškerých technických a programových prostředků osob jmenovaných ve Varování NÚKIB, (…);*
- *z jakého důvodu bylo nezbytné vyloučit skutečně veškeré technické a programové prostředky osob jmenovaných ve Varování NÚKIB, (…);*

- *jaká jiná opatření ke snížení rizik identifikovaných v analýze rizik Zadavatel zvažoval a z jaké důvodu se taková jiná – méně soutěž omezující – opatření nejeví jako dostatečná.“*.

21. Navrhovatel dále podotýká, že *„ani v rámci Stěžovateli dostupné dokumentace veřejné zakázky není k dispozici analýza rizik, na kterou Zadavatel v kontextu napadené zadávací podmínky odkazuje, a nelze tak přezkoumat pravdivost tvrzení Zadavatele, že dotčená podmínka souvisí s analýzou rizik, stejně tak, jako nelze přezkoumat, zda v daném případě skutečně nebylo možné aplikovat jiné – méně soutěž omezující – opatření ke snížení rizik údajně identifikovaných v analýze rizik, považuje Stěžovatel celé zadávací řízení za netransparentní a tudíž nezákonné, odporující ustanovení § 6 ZZVZ.“*., přičemž, jak navrhovatel dále uvádí, *„požadavek na zdůvodnění soutěž omezující Zadávací podmínky vyplývá přímo z dikce § 36 odst. 1 ZZVZ, kdy je nezákonné stanovit bezdůvodnou překážku hospodářské soutěže.“*.

K rozporu se zásadou zákazu diskriminace a přiměřenosti dle § 6 zákona

22. Navrhovatel ve svém návrhu namítá, že se zadavatel dopustil porušení zásady zákazu diskriminace a zásady rovného zacházení zakotvených v ustanovení § 6 odst. 2 zákona, když zadavatel dle navrhovatele *„stanovením Zadávacích podmínek bez řádného odůvodnění způsobil objektivní nemožnost určitých dodavatelů (jejichž technická řešení obsahují technické či programové prostředky Huawei) ucházet se o zakázku v předmětném zadávacím řízení, když ke snížení rizik údajně identifikovaných v analýze rizik, resp. k plnění povinností dle ZKB zvolil zcela nepřiměřené opatření v podobě úplného vyloučení veškerých technických a programových prostředků Huawei a ZTE (tj. výrobců uvedených ve Varování NÚKIB).“*.

23. Navrhovatel uvádí, že stanovením zadávací podmínky specifikované v odst. 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace hrozí navrhovateli újma, neboť v důsledku stanovení této zadávací podmínky je navrhovateli znemožněno se účastnit předmětného zadávacího řízení, a to *„jak v roli dodavatele, tak roli poddodavatele.“*.

24. Na základě výše uvedeného navrhovatel navrhuje, aby Úřad zrušil zadávací řízení na předmětnou veřejnou zakázku.

II. PRŮBĚH SPRÁVNÍHO ŘÍZENÍ

25. Úřad obdržel předmětný návrh dne 23. 9. 2019 a tímto dnem bylo podle ustanovení § 249 zákona ve spojení s § 44 odst. 1 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „správní řád“) zahájeno správní řízení o přezkoumání úkonů zadavatele.

26. Účastníky správního řízení podle § 256 zákona jsou:

- zadavatel,
- navrhovatel.

27. Zahájení správního řízení oznámil Úřad jeho účastníkům přípisem č. j. ÚOHS-S0358/2019/VZ-26216/2019/512/KMo ze dne 25. 9. 2019, který byl zadavateli i navrhovateli doručen téhož dne.

28. Dne 3. 10. 2019 bylo Úřadu doručeno nedatované vyjádření zadavatele k podanému návrhu na zahájení správního řízení o přezkoumání úkonů zadavatele a rovněž část dokumentace o zadávacím řízení.

Nedatované vyjádření zadavatele

29. Zadavatel ve svém vyjádření v prvé řadě předesílá, *„že stěžovatel v podaném návrhu pouze opakuje obsah námitek ze dne 28. 8. 2019[1]. S těmito argumenty se zadavatel – dle svého přesvědčení – zevrubně vypořádal ve svém rozhodnutí o námitkách ze dne 12. 9. 2019. Samotný obsah tohoto rozhodnutí pak návrhová argumentace reflektuje pouze zcela okrajově a lze tak konstatovat, že podaný návrh neobsahuje nad rámec námitek ze dne 28. 8. 2019 v zásadě nic nového (…).“*.

30. Zadavatel v této souvislosti v obecné rovině konstatuje, *„že setrvává na svém názoru vyjádřeném již v rozhodnutí o námitkách.“* a dále pak uvádí, že *»[n]ad tento rámec pak zadavatel Úřadu pro ochranu hospodářské soutěže (dále jen „úřad“) předkládá doklady a informace ke svému postupu při stanovení zadávacích podmínek, konkrétně pak při zpracování analýzy rizik postupem dle vyhl. č. 82/2018 Sb., o kybernetické bezpečnosti.«*, přičemž zadavatel považuje tyto informace s ohledem na zajištění bezpečnosti *„za utajované části mající charakter skutečností tvořících obchodní tajemství zadavatele (…)“*.

K omezení hospodářské soutěže nad míru nezbytně potřebnou k plnění povinností dle ZKB

31. Ohledně námitky navrhovatele, že zadavatel stanovením zadávací podmínky uvedené v odst. 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace porušil zákon, kdy navrhovatel argumentuje tím, že zadavatel paušálním, resp. úplným vyloučením technologií dotčených dvou společností překročil rámec výjimky stanovené v ustanovení § 4 odst. 4 zákona o kybernetické bezpečnosti, resp. v daném konkrétním případě podmínek varování NÚKIB vydaného postupem dle citovaného zákona, a dále pak, že zadavatel *»stanovil danou omezující podmínku „od stolu“ aniž zvážil alternativní možnosti řešení, neboť rizika plynoucí z možnosti aplikace technologií např. spol. Huawei mohou být „eliminována přijetím odpovídajících (dodatečných) technických opatření, která může být dodavatel zavázán na své náklady, resp. v rámci plnění veřejné zakázky, provést (např. redundance, ochrana skrze produkty třetích osob apod.).«*, zadavatel konstatuje, že návrh ani námitky navrhovatele, *„nijak nepolemizují s tím, že zadavatel byl na základě varování NÚKIB vydaného dne 17. 12. 2018 povinen ve smyslu ust. § 4 odst. 4 zákona o kybernetické bezpečnosti omezit využitelnost technologií společností Huawei a ZTE pro plnění veřejné zakázky.“*, nýbrž dle zadavatele navrhovatel polemizuje *„primárně pouze s rozsahem, v jakém zadavatel použitelnost těchto technologií vyloučil, a sekundárně s postupem, jakým zadavatel ke stanovení této zadávací podmínky dospěl.“*.

32. Zadavatel pak v této souvislosti uvádí, že *„předmět plnění této veřejné zakázky je součástí širšího záměru zadavatele vybudovat svoji informační infrastrukturu na základě hierarchicky uspořádaného M.T.B.M. modelu (…).“*.

33. V další části svého vyjádření zadavatel v podrobnostech popisuje, z čeho se výše uvedený model skládá a jaké má funkční vlastnosti a poukazuje na skutečnost, *„že systém provozovaný zadavatelem, do něhož má být předmět veřejné zakázky začleněn, využívají*

[1] Správně má být „ze dne 26. 8. 2019“ – pozn. Úřadu

orgány veřejné moci (…). Nad rámec toho se tento systém využívá i k přístupům do významných informačních systémů orgánů státní správy (…) nebo systémů Ministerstva vnitra ČR, které jsou kritickou informační infrastrukturou státu (…).“.

34. Zadavatel dále uvádí, že nesouhlasí s názorem navrhovatele, kdy dle navrhovatele, ohledně rizik z pohledu kybernetické bezpečnosti, zákon jakož i zákon o kybernetické bezpečnosti *„sledují stejné cíle, tj. maximální zachování hospodářské soutěže.“*.

35. Zadavatel ve svém návrhu zdůrazňuje, že *„[z]atímco ZZVZ stanovuje jako základní povinnost zadavatele zajistit efektivní soutěž o veřejnou zakázku a (kyber) bezpečnostní hledisko konstituuje až sekundárně jako výjimku z tohoto obecného přístupu. Zcela opačně zákon o kybernetické bezpečnosti zadavateli stanovuje jako základní cíl, (…), především udržení kybernetické bezpečnosti jím provozované infrastruktury, přičemž – zcela odlišně od ZZVZ – umožňuje pro naplnění tohoto účelu i výslovným zákonným zmocněním omezit hospodářskou soutěž (…)“* a dle zadavatele je *„primární“* povinností zadavatele dle zákona o kybernetické bezpečnosti *„provádět postupem dle § 5 vyhlášky o kybernetické bezpečnosti řízení rizik a v jeho rámci zjištěná rizika analyzovat, hodnotit a přijmout odpovídající bezpečnostní opatření, tj. opatření organizační a technická k jejich snížení na akceptovatelnou úroveň či eliminaci.“*.

36. Zadavatel dále popisuje, jaké povinnosti pro něj vyplývají ze zákona o kybernetické bezpečnosti a z vyhlášky o kybernetické bezpečnosti a odkazuje na *„výsledek výzkumu provedeného NÚKIB k hodnocení výsledků vydaného varování.“*, ze kterého dle zadavatele vyplývá, *„že cíle zákona o kybernetické bezpečnosti naplňuje nejefektivněji pouze vyloučení rizikových prostředků.“*, a dále pak zadavatel zdůrazňuje, *„že na podkladě varování NÚKIB aktualizoval svoji analýzu rizik (…). Na základě této aktualizace pak tato rizika ve vztahu vyhodnotil jako kritická (…) a tedy neakceptovatelná.“*.

37. K námitce navrhovatele, že zadavatel navrhovateli *„neumožnil využití předmětných technologií ani částečně.“* zadavatel uvádí, že *„s ohledem na předmět této veřejné zakázky nepřipadal takovýto postup v úvahu. Předmětem veřejné zakázky je dodávka přepínačů pro dvě vrstvy systému zadavatele. Jedná se o kompaktní zařízení, která nelze nijak dělit. Jinak řečeno je takovýto postup pojmově vyloučen a námitka stěžovatele je proto irelevantní.“*.

38. K námitce navrhovatele, že *»měl zadavatel umožnit využití předmětných technologií za současné podmínky, že dodavatel implementuje dodatečná technická či kybernetickobezpečnostní opatření do nabízených řešení. Jako příklad uvádí dohledové systémy jiných výrobců, které by nebezpečnou technologii stěžovatele „hlídaly“.«,* zadavatel konstatuje, že *„takovýto postup není v daných podmínkách možný z hlediska technického, bezpečnostního, ostatně ani z hlediska účelnosti a efektivnosti vynakládaných prostředků na investici, kterou zadavatel k naplnění svých potřeb a legitimních zájmů nepotřebuje (…).“*.

39. Zadavatel ve svém vyjádření uvádí, že, jak již uvedl v rozhodnutí o námitkách, *„musel při analýze rizik, před kterými vydal NÚKIB dne 17. 12. 2018 své varování, přihlížet k jejich specifické povaze.“*, přičemž, jak dále uvádí, s odkazem na § 5 vyhlášky o kybernetické bezpečnosti *„je pak třeba připomenout, že zadavatel je povinen analyzovat a vyhodnotit rizika plynoucí (v daném případě) z těchto technologií a přijmout odpovídající opatření.“* a zdůrazňuje, že *„se v daném případě nejedná o situaci, kdy by bylo možné přijmout jen dílčí opatření (tj. omezení, nikoliv technologické vyloučení), a připustit použití technologií spol.*

Huawei a ZTE na plnění veřejné zakázky v určitém rozsahu.“, přičemž dále namítá, že není možné zadavateli přičítat k tíži, že *„zcela objektivně nemá možnosti, jak detailně (z interního pohledu) prozkoumat technologie spol. Huawei a ZTE, neboť se z podstaty věci nejedná o informace jakkoliv veřejně dostupné.“*.

40. K námitce navrhovatele, že *„ve vztahu k technologiím stěžovatele nebyly identifikovány žádné zranitelnosti, kterých by mohl využít, a hrozby.“,* zadavatel uvádí a zdůrazňuje, že v rámci stanovení zadávacích podmínek tyto zranitelnosti a hrozby identifikoval, přičemž ve svém vyjádření jejich výčet uvádí.

41. Zadavatel pak doplňuje, že při sestavování zadávacích podmínek *„důsledně postupoval jak dle ZZVZ, tak podle zákona o kybernetické bezpečnosti, prováděcí vyhlášky k němu a dále podle obsahu varování NÚKIB a jím vydané metodiky k tomuto varování (důvody nepřipuštění použití technologií spol. Huawei a ZTE byly učiněny součástí zadávacích podmínek, a to v odst. 5.3. zadávací dokumentace).“*.

42. Na podporu svých tvrzení zadavatel odkazuje a Úřadu doložil mj. tyto dokumenty a listiny s tím, že zadavatel dále s odkazem na ustanovení § 56 správního řádu navrhuje, *„aby si Úřad pro ochranu hospodářské soutěže k téže otázce, tedy k obsahu těchto listin a jejich souladu s vyhláškou o kybernetické bezpečnosti, vyžádal odborné vyjádření NÚKIB“*:

    1. „Studie stavu sítě Metropolnet a.s., návrh modernizace, monitoringu a správy sítě (PROJEKT 10): Specifikace Modelu M.T.B.M v rámci podání na ÚOHS“;

    2. „Analýza kyberbezpečnosti a bezpečnosti IS v rámci přípravy na certifikaci ISO 27000“ ze dne 13. 3. 2017;

    3. „Dílčí riziková analýza zaměřená na diskové pole a na aktivní síťové prvky v core vrstvě“ ze dne 28. 3. 2019 (vč. přílohové tabulky);

    4. „Dílčí aktualizace Projekt 10: Riziková analýza a další konsekvence kyberbezpečnosti ke dni 30. 6. 2019“.

    (dále jen „rozhodné dokumenty“)

    K nezákonnosti stanovení předmětné zadávací podmínky bez provedení komplexního hodnocení rizik dle ZKB, resp. VKB

43. K námitce navrhovatele, že zadavatel neprovedl *„komplexní“* hodnocení rizik ve smyslu ustanovení § 2 písm. d) vyhlášky o kybernetické bezpečnosti, a v důsledku toho je dle navrhovatele *„zadávací podmínka uvedená v čl. 5.3. zadávací dokumentace stanovená nezákonným způsobem.“,* zadavatel uvádí, že *„předmětem námitek, resp. návrhu směřujícího proti zadávacím podmínkám může být pouze obsah těchto zadávacích podmínek, popř. postup stanovený ZZVZ k jejich sestavení.“* a zadavatel je tak přesvědčen, že *„analýzu provedl správně a fundovaně, tedy v souladu s požadavky zákona o kybernetické bezpečnosti a podzákonného předpisu.“*.

    K rozporu se zásadou transparentnosti ve smyslu § 6 zákona

44. K námitce navrhovatele, že zadavatel tím, že *„zadávací podmínku uvedenou v bodě 5.3. zadávací dokumentace přímo v jejím textu neodůvodnil.“*, což navrhovatel považuje za porušení zásady transparentnosti, zadavatel uvádí a je přesvědčen, že *„zadávací podmínky*

vymezil v souladu se ZZVZ a opakuje, že ZZVZ nestanovuje zadavateli povinnost jednotlivé zadávací podmínky odůvodňovat (a to ani v § 36 odst. 1 ZZVZ).“.

K rozporu se zásadou zákazu diskriminace a přiměřenosti dle § 6 zákona

45. K námitce navrhovatele, že zadavatel *„paušálním vyloučením technologií výrobců Huawei a ZTE porušil zásady [zákazu] diskriminace a přiměřenosti ve smyslu § 6 zákona o zadávání veřejných zakázek.“* zadavatel uvádí a je toho názoru, že *„svůj postup považuje za zákonný, důvodný, aplikující povinnosti plynoucí ze zákona o kybernetické bezpečnosti a jeho prováděcího předpisu, jakož i varování NÚKIB, což založilo oprávněný důvod k vyloučení předmětných technologií v zadávacím řízení, a tedy v konečném důsledku stěžovatele. V důsledku uvedeného zadavatel postupoval tak, že neporušil ust. § 36 odst. 1 ZZVZ, ani zásady, na kterých ZZVZ spočívá (§ 6 ZZVZ).“*.

46. Závěrem svého vyjádření pak zadavatel navrhuje, aby Úřad podaný návrh v souladu s ustanovením § 265 písm. a) zákona zamítl *„jako nedůvodný“.*

Další průběh správního řízení

47. Usnesením č. j. ÚOHS-S0358/2019/VZ-27304/2019/512/KMo ze dne 7. 10. 2019 stanovil Úřad zadavateli lhůtu pěti dnů ode dne doručení tohoto usnesení k provedení úkonu – doručení kompletní originální dokumentace o zadávacím řízení na veřejnou zakázku.

48. Dne 10. 10. 2019 doručil zadavatel Úřadu další část dokumentace o zadávacím řízení na veřejnou zakázku.

49. Usnesením č. j. ÚOHS-S0358/2019/VZ-27868/2019/512/KMo ze dne 11. 10. 2019 stanovil Úřad zadavateli lhůtu k provedení úkonu, a to podání informace Úřadu o dalších úkonech, které zadavatel provede v šetřeném zadávacím řízení v průběhu správního řízení a zaslání příslušné dokumentace o zadávacím řízení.

50. Usnesením č. j. ÚOHS-S0358/2019/VZ-28013/2019/512/KMo ze dne 16. 10. 2019 Úřad správní řízení dle § 64 odst. 1 písm. e) správního řádu ve spojení s § 261 odst. 2 zákona přerušil s cílem získat odborné stanovisko příp. znalecký posudek k zadavatelem poskytnuté analýze rizik zpracované zadavatelem na základě varování NÚKIB, konkrétně k otázce, zda předmětná analýza rizik byla z formálního a obsahového hlediska provedena v souladu s dotčenými právními předpisy (zejména ZKB a VKB) a obecně platnými uznávanými standardy v oboru kybernetické bezpečnosti.

51. Úřad žádostí o sdělení odborného stanoviska č. j. ÚOHS-S0358/2019/VZ-28460/2019/512/KMo ze dne 17. 10. 2019 požádal NÚKIB o zaslání odborného stanoviska, zda je předmětná analýza rizik z formálního i obsahového hlediska provedená zadavatelem v souladu s dotčenými právními předpisy, zejm. ZKB a VKB a obecně platnými uznávanými standardy v oboru kybernetické bezpečnosti (dále jen „žádost o sdělení odborného stanoviska“).

52. Úřad přípisem s názvem „Oznámení o pokračování správního řízení“ č. j. ÚOHS-S0358/2019/VZ-30811/2019/512/KMo ze dne 12. 11. 2019 účastníkům správního řízení oznámil, že ve správním řízení se pokračuje, a to za účelem vydání rozhodnutí o nařízení předběžného opatření spočívajícího v uložení zákazu zadavateli uzavřít smlouvu v předmětném zadávacím řízení, a to až do pravomocného skončení správního řízení.

53. Dne 12. 11. 2019 Úřad rozhodnutím č. j. ÚOHS-S0358/2019/VZ-30824/2019/512/KMo nařídil předběžné opatření, kterým zadavateli zakázal uzavřít v zadávacím řízení na veřejnou zakázku smlouvu na plnění veřejné zakázky.

54. Usnesením č. j. ÚOHS-S0358/2019/VZ-30842/2019/512/KMo ze dne 18. 11. 2019 Úřad správní řízení dle § 64 odst. 1 písm. e) správního řádu ve spojení s § 261 odst. 2 zákona opětovně přerušil s cílem získat odborné stanovisko, příp. znalecký posudek k zadavatelem poskytnuté analýze rizik zpracované zadavatelem na základě varování NÚKIB, a sice zda předmětná analýza rizik byla z formálního a obsahového hlediska provedena v souladu s dotčenými právními předpisy, zejm. ZKB a VKB a obecně platnými uznávanými standardy v oboru kybernetické bezpečnosti.

55. Dne 25. 11. 2019 obdržel Úřad od NÚKIB přípis s názvem „Sdělení k postupu společnosti Metropolnet, a.s.“ ze dne 25. 11. 2019 (dále je „stanovisko NÚKIB“).

Stanovisko NÚKIB ze dne 25. 11. 2019

56. NÚKIB ve svém stanovisku v prvé řadě rekapituluje, jaké rozhodné dokumenty (blíže viz bod 43. odůvodnění tohoto rozhodnutí) mu byly Úřadem doručeny s žádostí Úřadu o jeho vyjádření, zda jsou tyto rozhodné dokumenty, zpracované zadavatelem, podle jeho odborného názoru z formálního i obsahového hlediska v souladu s dotčenými právními předpisy (zejména ZKB a VKB) a obecně platnými a uznávanými standardy v oboru kybernetické bezpečnosti.

57. V této souvislosti NÚKIB poznamenává, že si od zadavatele vyžádal další dokument, který dle NÚKIB nebyl součástí rozhodných dokumentů, které NÚKIB od Úřadu obdržel, a to konkrétně *„přílohová tabulka obsahující kompletní analýzu rizik zaměřenou na diskové pole a na aktivní síťové prvky v core vrstvě“*, přičemž, jak NÚKIB uvádí, jedná se o dokument s názvem „Dílčí hodnocení rizik ZoKB_pro diskové pole a síťové prvky“. Dále pak NÚKIB uvádí, že od zadavatele obdržel spolu s tímto dokumentem i další dokumenty, které dle vyjádření NÚKIB *„obsahují obecné hodnocení rizik pro vybrané systémy spravované zadavatelem bez přímé návaznosti na vydání varování NÚKIB ze dne 17. 12. 2018 a posloužily jako podpůrné materiály pro vypracování tohoto stanoviska.“*.

58. NÚKIB ve svém stanovisku upozorňuje na skutečnost, že v současné době neeviduje společnost Metropolnet, a.s. (zadavatele) jako povinnou osobu podle § 3 zákona o kybernetické bezpečnosti a do dnešního dne *„nevydal žádné rozhodnutí nebo opatření obecné povahy, kterým by zadavatele určil povinnou osobou podle § 3 ZBK, a žádné řízení o určení v současné době nevede. (…) zadavatel do dnešního dne neinformoval NÚKIB o tom, že by byl některou z povinných osob, u kterých dochází k tzv. samourčení (…).“*, přičemž dle vyjádření NÚKIB *„[a]ni Statutární město Ústí nad Labem není povinnou osobou podle § 3 ZKB (ani na základě rozhodnutí NÚKIB, ani na základě samourčení)* [2] *“*.“

59. Dle NÚKIB tak lze uzavřít, *„že pokud není zadavatel povinnou osobou dle ZKB, nelze u něj dovodit ani povinnost postupovat podle pravidel obsažených v ZKB.“*, což dle vyjádření NÚKIB

[2] V této souvislosti NÚKIB odkazuje na znění odst. 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace, kde zadavatel mj. uvedl, že *„v rámci svých činností technicky zajišťuje chod sítě a provoz informačních systémů Statutárního města Ústí nad Labem, vč. Magistrátu Statutárního města Ústí nad Labem (…).“* – pozn. Úřadu

neznamená, *„že by zadavatel nemohl aplikovat ustanovení ZKB a VKB ve svých strukturách dobrovolně, např. z důvodu, že to po něm požadují jeho smluvní partneři nebo jeho zřizovatel, nebo z důvodu, že zadavatel usiluje o získání certifikace ISO 27000 (celá koncepce VKB je založena právě na normě ISO 27001). (…).“* a dle NÚKIB, zadavatel dovozuje svou povinnost zajišťovat bezpečnost informací podle ZKB ze skutečnosti, že přistupuje do systémů, které musejí požadavky ZKB splňovat. Taková povinnost zadavateli *„sice neplyne ze zákona (ZKB, resp. VKB pouze stanoví povinným osobám povinnost řídit své dodavatele), (…).“*.

60. NÚKIB dále ve svém sdělení konstatuje, že varování NÚKIB ze dne 17. 12. 2018 *„samo o sobě neukládá žádné povinnosti, stejně jako není určeno pouze omezenému okruhu adresátů. Speciální ustanovení ZKB a VKB stanoví, které orgány a osoby (povinné osoby) mají zákonnou povinnost zohlednit varování v procesu řízení rizik.“*, ovšem, jak NÚKIB dále uvádí, lze předpokládat, že i orgány a osoby, které nespadají do působnosti ZKB, budou s informací obsaženou ve varování NÚKIB v rámci řízení bezpečnosti svých informačních systémů dále pracovat a budou ji zohledňovat v procesu řízení rizik.

61. V případě samotného posouzení souladnosti postupu zadavatele při tvorbě analýzy rizik s ustanoveními ZKB a VKB, NÚKIB upozorňuje, že obsah analýzy rizik a způsob jejího provedení je třeba posuzovat *„i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik.“*. V této souvislosti NÚKIB konstatuje, že *„hodnocení rizik zadavatelem, jak bylo v předložených dokumentech prezentováno, ve vztahu ke konkrétní veřejné zakázce neodpovídá požadavkům stanoveným v ZKB a VKB zejm. shledává jako nedostatečnou identifikaci primárních a podpůrných aktiv a vazeb mezi nimi, (…).“*.

62. NÚKIB je tak přesvědčen, že postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření *„je tedy z pohledu NÚKIB nedostatečně zdokumentován a je obecně (pro nezainteresovanou osobu) neopakovatelný a zmatečný.“* a dle NÚKIB pak postup zadavatele *„nelze označit za souladný se ZKB a VKB.“*

63. Co se týče hodnocení souladnosti postupu zadavatele s pravidly obsaženými v normě ISO 27001, to dle vyjádření NÚKIB není v jeho kompetenci (…). V této souvislosti pak NÚKIB upřesňuje, že je *„pověřen dozorováním dodržování ZKB a VKB, nikoli norem řady ISO 27000, (…).“*.

64. Na základě zadavatelem předložených dokumentů NÚKIB uzavírá, že výběr bezpečnostního opatření *„se nezakládá na hodnocení rizik provedených zcela v souladu s požadavky ZKB a VKB.“*.

Další průběh správního řízení

65. Úřad přípisem s názvem „Oznámení o pokračování správního řízení“ č. j. ÚOHS-S0358/2019/VZ-32820/2019/512/KMo ze dne 28. 11. 2019 účastníkům správního řízení oznámil, že ve správním řízení se pokračuje, jelikož dne 25. 11. 2019 odpadla překážka, pro kterou bylo předmětné správní řízení přerušeno.

66. Usnesením č. j. ÚOHS-S0358/2019/VZ-33438/2019/512/KMo ze dne 4. 12. 2019 stanovil Úřad účastníkům řízení lhůtu 7 dnů ode dne doručení tohoto usnesení, ve které se mohli vyjádřit k podkladům rozhodnutí, přičemž dané usnesení bylo navrhovateli i zadavateli doručeno dne 4. 12. 2019.

67. Dne 11. 12. 2019 obdržel Úřad od zadavatele nedatovaný přípis s názvem „Vyjádření k podkladům po nahlédnutí do spisu“.

68. Navrhovatel se ve stanovené lhůtě, ani později, k podkladům rozhodnutí nevyjádřil.

Nedatované vyjádření zadavatele k podkladům pro rozhodnutí

69. Zadavatel se ve svém vyjádření postupně vyjadřuje ke skutečnostem a závěrům uvedeným ve stanovisku NÚKIB ze dne 25. 11. 2019, které bylo Úřadu doručeno téhož dne.

70. Ohledně skutečnosti, kdy NÚKIB ve svém stanovisku uvádí, že v současné době neeviduje společnost Metropolnet, a.s. jako osobu povinnou dle ustanovení § 3 zákona o kybernetické bezpečnosti, zadavatel konstatuje, *„že bude prostřednictvím vlastní WAN/LAN sítě připojovat do sítě KIVS a CMS (jejichž provozovatel, tj. MV ČR je povinnou osobou), a proto dobrovolně přistoupil k aplikaci vybraných povinností dle ZKB/VKB“*, přičemž dále upřesňuje, že do prostředí CMS (Centrální místo služeb – pozn. Úřadu) a KIVS (komunikační infrastruktura veřejné správy – pozn. Úřadu) se Statutární město Ústí nad Labem bude připojovat v roce 2020, a podle zadavatele, tak Statutární město Ústí nad Labem *„bude v tu chvíli plně odevzdané do rukou MVČR, které je dle ZKB a VKB povinno vyžadovat a prosazovat dodržování bezpečnostních směrnic po všech připojených subjektech.“*.

71. V další části svého vyjádření zadavatel popisuje a poukazuje na „Informační koncepce České republiky (v gesci Ministerstva vnitra)“, „Program Digitální Česko – Úvodní dokument“, „Sněmovní tisk 447 – N.z. o právu na digitální služby“, „Směrnice RŽP MPO“, „Metamodel bezpečnostní architektury“ a v neposlední řadě na „Odpovědnost vůči ZOK“, přičemž v této souvislosti odkazuje na příslušné zdroje, ze kterých vycházel.

72. Zadavatel dále objasňuje, že, jak již zmínil NÚKIB ve svém stanovisku, není evidován jako povinná osoba dle ZKB a VKB *a „není ani plně v souladu s touto metodikou, co se týče interních směrnic, zejména z důvodu obrovské procesní a finanční zátěže, která je se zajištěním plného souladu s ZKB/VKB spojená. Riziková analýza však byla dle ZKB vypracována, a co hlavně i dle ISO 27001, na kterou se zadavatel plánuje certifikovat (…).“*.

73. Závěrem pak zadavatel shrnuje, že *„neomezuje soutěž záměrně a svévolně, ale má k tomu jednoznačný důvod – nejistotu na trhu, AVIZOVANÝ dopad na kybernetickou bezpečnost (na kterou upozorňuje nejvyšší státní instituce v této oblasti – Národní úřad pro kybernetickou a informační bezpečnost) a ochranu své investice v budoucnosti.“*, přičemž dále zdůrazňuje, že chtěl omezením veřejné soutěže předejít *„vlastní analýzou zjištěným rizikům v oblasti kybernetické bezpečnosti, minimalizovat rizika jejich dopadu a vyhnout se bezpečnostním i ekonomickým dopadům v budoucnu.“*, avšak, jak zadavatel dále uvádí, nepopírá, že *„nepostupoval jednoznačně v souladu s požadavky ZKB/VKB (na úrovni metodické), ale podstatná rizika identifikoval a svým postupem je snížil na akceptovatelnou úroveň“* s tím, že dále považuje za nezbytné zdůraznit, že *„jako veřejný subjekt z hlediska zajištění vysoké úrovně kybernetické bezpečnosti v České republice a Statutárního města Ústí nad Labem soustavně a dlouhodobě pracoval a pracuje na zajištění kybernetické bezpečnosti ve vztahu k upozornění k tomu zřízenému státnímu úřadu a upozornění tohoto státního úřadu na potenciálně nebezpečné čínské technologie.“*.

III. ZÁVĚRY ÚŘADU

74. Úřad přezkoumal na základě ustanovení § 248 a následujících ustanovení případ ve všech vzájemných souvislostech a po zhodnocení všech podkladů pro rozhodnutí, zejména relevantních částí obdržené dokumentace o zadávacím řízení, stanovisek předložených účastníky správního řízení a na základě vlastního zjištění rozhodl o tom, že zadavatel stanovil zadávací podmínky v zadávacím řízení na předmětnou veřejnou zakázku v rozporu s ustanovením § 36 odst. 1 zákona ve spojení se zásadou zákazu diskriminace zakotvenou v ustanovení § 6 odst. 2 zákona tím, že stanovil zadávací podmínky tak, že vytvářely bezdůvodné překážky hospodářské soutěže, když v článku 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace, mj. stanovil, že vylučuje technické a programové prostředky dotčených společností z předmětného zadávacího řízení, a to s odvoláním na „Varování č. j. 3012/2018-NÚKIB-E/110“ ze dne 17. 12. 2018 a „Metodiku k varování ze dne 17. prosince 2018“ ze dne 4. 1. 2019 vydanými Národním úřadem pro kybernetickou a informační bezpečnost, ačkoliv neexistovaly relevantní důvody na straně zadavatele pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu výše uvedené technické a programové prostředky, a zadavatel tak nedodržel zásadu zákazu diskriminace ve vztahu k navrhovateli.

75. Ke svému rozhodnutí uvádí Úřad následující rozhodné skutečnosti.

K postavení zadavatele

76. Pro řádné prošetření případu považuje Úřad za vhodné identifikovat kategorii zadavatele veřejné zakázky.

77. Podle § 4 odst. 4 zákona pokud zadavatel podle § 4 odst. 1 až 3 zákona zahájí zadávací řízení, i když k tomu nebyl povinen, je povinen ve vztahu k zadávané veřejné zakázce dodržovat tento zákon.

78. Podle § 4 odst. 5 zákona se za zadavatele považuje také jiná osoba, která zahájila zadávací řízení, ačkoliv k tomu nebyla povinna, a to ve vztahu k tomuto zadávacímu řízení a do jeho ukončení.

79. Vzhledem k tomu, že zadavatel (Metropolnet, a.s.) zahájil dne 23. 9. 2019 odesláním oznámení o zahájení zadávacího řízení k uveřejnění předmětné zadávací řízení, nemůže být v daném případě sporu o jeho povinnosti dodržovat ve vztahu k předmětné veřejné zakázce zákon, a to už jen s ohledem na znění ustanovení § 4 odst. 4 a 5 zákona.

K výroku I. tohoto rozhodnutí

Relevantní ustanovení zákona a jiných právních předpisů

80. Podle § 6 odst. 1 zákona zadavatel při postupu podle tohoto zákona musí dodržovat zásady transparentnosti a přiměřenosti.

81. Podle § 6 odst. 2 zákona musí zadavatel ve vztahu k dodavatelům dodržovat zásadu rovného zacházení a zákazu diskriminace.

82. Podle § 28 odst. 1 písm. a) zákona se pro účely zákona zadávacími podmínkami rozumí veškeré zadavatelem stanovené

1. podmínky průběhu zadávacího řízení,

2. podmínky účasti v zadávacím řízení,

3. pravidla pro snížení počtu účastníků zadávacího řízení nebo snížení počtu předběžných nabídek nebo řešení,

4. pravidla pro hodnocení nabídek,

5. další podmínky pro uzavření smlouvy na veřejnou zakázku podle § 104 zákona.

83. Podle § 36 odst. 1 zákona nesmí být zadávací podmínky stanoveny tak, aby určitým dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže.

84. Podle § 2 písm. d) zákona o kybernetické bezpečnosti se rozumí významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

85. Podle § 2 písm. g) zákona o kybernetické bezpečnosti se rozumí provozovatelem informačního nebo komunikačního systému orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém.

86. Podle § 3 zákona o kybernetické bezpečnosti jsou orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),

c) správce a provozovatel informačního systému kritické informační infrastruktury,

d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,

f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),

g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a

h) poskytovatel digitální služby.

87. Podle § 2 písm. i) vyhlášky o kybernetické bezpečnosti se rozumí řízením rizik činnost zahrnující hodnocení rizik, výběr a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik.

88. Podle § 2 písm. n) vyhlášky o kybernetické bezpečnosti se rozumí významným dodavatelem provozovatel informačního nebo komunikačního systému (dále jen "provozovatel") a každý, kdo s povinnou osobou vstupuje do právního vztahu, který je významný z hlediska bezpečnosti informačního a komunikačního systému.

89. Podle § 5 odst. 1 písm. a) vyhlášky o kybernetické bezpečnosti povinná osoba v rámci řízení rizik v návaznosti na § 4 stanoví metodiku pro hodnocení rizik, včetně stanovení kritérií pro akceptovatelnost rizik.

Zjištěné skutečnosti

Varování Národního úřadu pro kybernetickou a informační bezpečnost

90. Úřad na tomto místě uvádí, že dne 17. 12. 2018 bylo Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) vydáno Varování č. j. 3012/2018-NÚKIB-E/110 dle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“ či „zákon o kybernetické bezpečnosti“), ve kterém NÚKIB varuje před použitím technických nebo programových prostředků společnosti Huawei Technologies Co., Ltd., Šen-Čen, Čínská lidová republika, a společnosti ZTE Corporation, Šen-Čen, Čínská lidová republika, včetně jejich dceřiných společností (dále jen „dotčené společnosti“), neboť představují hrozbu v oblasti kybernetické bezpečnosti (dále jen „varování NÚKIB“). K tomuto varování NÚKIB vydal dne 4. 1. 2019 metodiku, která konkretizuje možné postupy správců informačních a komunikačních systémů spadajících pod ZKB, dále vysvětluje institut varování, popisuje princip řízení rizik a nastiňuje možnosti při zajištění plnění povinností podle ZKB v souladu s předpisy regulujícími zadávaní veřejných zakázek (dále jen „metodika NÚKIB“).

91. V odst. 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace je uvedeno následující:

»Zadavatel v rámci svých činností technicky zajišťuje chod sítě a provoz informačních systémů Statutárního města Ústí nad Labem vč. Magistrátu Statutárního města Ústí nad Labem (dále také „MMÚL“), úřadů městských částí a dalších organizací zřizovaných MMÚL.

Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) jako ústřední správní orgán pro kybernetickou bezpečnost podle § 12 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (dále jen „ZoKB“) varování č. j. 3012/2018-NÚKIB-E/110, kde stanovil, že použití technických prostředků nebo programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:

- *Huawei Technologies Co., Ltd., Šen-Čen, Čínská lidová republika*
- *ZTE Corporation, Šen-Čen, Čínská lidová republika.*

Dne 4. ledna 2019 vydal NÚKIB Metodiku k varování ze dne 17. prosince 2018 Verze 1.0 (dále jen „metodika“), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou zadavatel provedl analýzu rizik související s plánovaným zadávacím řízením na dodávku – obnovu páteřní a přístupové infrastruktury. V návaznosti na to zadavatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky zmíněných společností jako neakceptovatelná, a tedy v souladu se svými interními postupy jako nepřípustná. Tato skutečnost pak determinuje další postup zadavatele.

Zadavatel nemá bližší informace o konkrétní podobě hrozby, kterou prostředky uvedených společností podle varování NÚKIB představují, a není tak objektivně schopen přijmout žádné jiné bezpečnostní opatření (než níže uvedené), které by prokazatelně a v dostatečné míře

eliminovalo identifikované bezpečnostní riziko. Z důvodu obligatorně stanovené míry hrozby při využití technických a programových prostředků uvedené ve varování NÚKIB a související metodice tedy snížení rizika spojeného s používáním technických a programových prostředků dotčených společností nelze dosáhnout jinak než vyloučením technických a programových prostředků těchto společností z používání v informačních a komunikačních systémech zadavatele, a tím i jejich vyloučením z tohoto zadávacího řízení.

V souladu s § 4 odst. 4 ZoKB zadavatel zohledňuje požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro zadavatelem zajišťované informační nebo komunikační systémy. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěže.

Na základě varování NÚKIB, navazující metodiky a zadavatelem provedené analýzy rizik, ve spojení s ust. § 4 odst. 4 ZoKB, tedy není možné technické a programové prostředky výše uvedených společností v nabídkách účastníků (včetně jejich poddodavatelů) akceptovat.«

(dále jen „sporná podmínka“ či „sporné opatření“)

92. Na základě žádosti o sdělení odborného stanoviska ze dne 17. 10. 2019, Úřad obdržel dne 25. 11. 2019 stanovisko NÚKIB, kde je uvedeno následující.

NÚKIB v prvé řadě uvádí, že součástí rozhodných dokumentů, které obdržel od Úřadu, nebyla *„přílohová tabulka obsahující kompletní analýzu rizik zaměřenou na diskové pole a na aktivní síťové prvky v core vrstvě“*, kterou si následně od zadavatele vyžádal, přičemž se jednalo o dokument s názvem „Dílčí hodnocení rizik ZoKB_pro diskové pole a síťové prvky“ s tím, že, jak NÚKIB dále uvedl, spolu s tímto dokumentem obdržel od zadavatele další dokumenty, a to konkrétně dokumenty pod názvem „Hodnocení rizik ZoKB_pro VIS final“, „Hodnocení rizik ISO27000 final“ a „Metropolnet – komentář tabulky rizik shrnutí_v5 – prijate rev“ s tím, že dle NÚKIB tyto dokumenty *„obsahují obecné hodnocení rizik pro vybrané systémy spravované zadavatelem bez přímé návaznosti na vydání varování NÚKIB ze dne 17. 12. 2018 a posloužily jako podpůrné materiály pro vypracování tohoto stanoviska.“* (dále jen „další rozhodné dokumenty“).

NÚKIB ve svém stanovisku upozorňuje na skutečnost, že »*v současné době neeviduje společnost Metropolnet, a.s. jako povinnou osobu podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“). NÚKIB do dnešního dne nevydal žádné rozhodnutí nebo opatření obecné povahy, kterým by zadavatele určil povinnou osobou podle § 3 ZKB, a žádné řízení o určení v současné době nevede. Stejně tak zadavatel do dnešního dne neinformoval NÚKIB o tom, že by byl některou z povinných osob, u kterých dochází k tzv. samourčení (tzn. povinnou osobou se subjekt stává ze zákona naplněním definičních znaků a je automaticky povinen nahlásit NÚKIB své kontaktní údaje). NÚKIB nadto ani nedisponuje informacemi, na základě kterých by získal důvodné podezření, že zadavatel je povinnou osobou podle § 3 ZKB a v rozporu se zákonem své kontaktní údaje nenahlásil.«*

NÚKIB ve svém stanovisku dále uvádí, že ani Statutární město Ústí nad Labem, pro které zadavatel, tak jak je uvedeno v odst. 5.3. zadávací dokumentace, v rámci svých činností technicky zajišťuje chod sítě a provoz informačních systémů *»není povinnou osobou podle § 3 ZKB (ani na základě rozhodnutí NÚKIB, ani na základě samourčení) a zejm. s ohledem na*

počet obyvatel Statutárního města Ústí nad Labem a skutečnost, že obce nemohou být správci významných informačních systémů ve smyslu § 2 písm. d) a § 3 písm. e) ZKB, nelze předpokládat, že by se Statutární město Ústí nad Labem mělo v dohledné době povinnou osobou stát. Zadavatel tedy v současné době není ani provozovatelem informačního nebo komunikačního systému povinné osoby ve smyslu § 2 písm. g) ZKB [ani významným dodavatelem ve smyslu § 2 písm. n) vyhlášky č. 82/2018 Sb., bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), dále jen „VKB"].«

V této souvislosti pak NÚKIB uzavírá, *„že pokud není zadavatel povinnou osobou podle ZKB, nelze u něj dovodit ani povinnost postupovat podle pravidel obsažených v ZKB."* Podle NÚKIB právě uvedené ovšem neznamená, *„že by zadavatel nemohl aplikovat ustanovení ZKB a VKB ve svých strukturách dobrovolně, např. z důvodu, že to po něm požadují jeho smluvní partneři nebo jeho zřizovatel, nebo z důvodu, že zadavatel usiluje o získání certifikace ISO 27000 (celá koncepce VKB je založena právě na normě ISO 27001)."*.

NÚKIB dále uvádí, že zadavatel na str. 4 dokumentu „Dílčí riziková analýza zaměřená na diskové pole a aktivní síťové prvky v core vrstvě" uvádí, že *»„[s]polečnost Metropolnet zajišťuje přístup přes síť MVČR ke kritické infrastruktuře státu z pohledu zákona o kybernetické bezpečnosti (KIVS = komunikační infrastruktura veřejné správy, CMS = centrální místo služeb). Tudíž je nutné, aby požadavky kladené na Kritickou infrastrukturu MV splňovala i firma Metropolnet, tj. prakticky naplňovala požadavky Kybernetického zákona".*« Podle NÚKIB tak zadavatel *„dovozuje svou povinnost zajišťovat bezpečnost informací podle ZKB ze skutečnosti, že přistupuje do systémů, které musejí požadavky ZKB splňovat."*. K tomu NÚKIB konstatuje, že taková povinnost zadavateli *„sice neplyne ze zákona (ZKB, resp. VKB pouze stanoví povinným osobám povinnost řídit své dodavatele), nicméně uvedený požadavek může být obsažen v podmínkách provozování citovaných systémů Ministerstva vnitra, resp. může být předmětem dalších smluvních ujednání mezi zadavatelem a Ministerstvem vnitra (jejich obsah však NÚKIB není znám)."*.

K zohlednění varování NÚKIB ze dne 17. 12. 2018 zadavatelem pak NÚKIB uvádí, *„že varování ve smyslu § 12 ZKB je aktem s obecnou platností, kterým NÚKIB informuje širokou veřejnost o existenci hrozby v oblasti kybernetické bezpečnosti. Varování samo o sobě neukládá žádné povinnosti, stejně jako není určeno pouze omezenému okruhu adresátů. Speciální ustanovení ZKB a VKB stanoví, které orgány a osoby (povinné osoby) mají zákonnou povinnost zohlednit varování v procesu řízení rizik. Lze však předpokládat (…), že i orgány a osoby, které nespadají do působnosti ZKB, budou s informací obsaženou ve varování v rámci řízení bezpečnosti svých informačních systémů dále pracovat a budou ji zohledňovat v procesu řízení rizik. Jak VKB, tak norma ISO 27001 totiž požadují, aby povinné osoby, resp. subjekty aplikující normu, při řízení rizik zohledňovaly jim známé relevantní hrozby."*.

Ohledně samotného posouzení souladnosti postupu zadavatele při tvorbě analýzy rizik s ustanoveními ZKB a VKB, NÚKIB v prvé řadě uvádí, že *„obsah analýzy rizik a způsob jejího provedení je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik. Proces řízení rizik sestává z hodnocení rizik (jehož součástí je identifikace, analýza a vyhodnocení rizik), výběru a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) VKB]. Výběr*

konkrétního bezpečnostního opatření, jehož implementace sníží hodnotu rizika na akceptovatelnou úroveň, pak musí být založen nikoli pouze na samotné analýze rizik (jejímž výsledkem je striktně vzato pouze stanovení hodnoty rizika), nýbrž i na navazujícím vyhodnocení rizik (tedy určení, zda je riziko akceptovatelné či nikoli) a zvážení v úvahu přicházejících bezpečnostních opatření. (…) Pro posouzení správnosti postupu povinné osoby při tvorbě analýzy rizik je krom jiného nezbytné i posouzení toho, zda celý proces hodnocení rizik, do něhož tvorba analýzy rizik spadá a od jehož zbylých součástí je funkčně neoddělitelná, byl proveden v souladu s metodikou k tomu vyhotovenou [srov. § 5 odst. 1 písm. a) VKB].“.

NÚKIB dále uvádí, že *„[p]o prostudování poskytnutých dokumentů NÚKIB konstatuje, že hodnocení rizik zadavatelem, jak bylo v předložených dokumentech prezentováno, ve vztahu ke konkrétní veřejné zakázce neodpovídá požadavkům obsaženým v ZKB a VKB.“*. Jako nedostatečnou NÚKIB shledává zejména *„identifikaci primárních a podpůrných aktiv a vazeb mezi nimi, výběr konkrétních podpůrných aktiv, na základě jejichž hodnocení došlo k zákazu použití prostředků dotčených obchodních společností v zadávacím řízení, dále lze identifikovat určitou zmatečnost a nejednotnost v popisu stupnic pro hodnocení jednotlivých proměnných vzorce pro výpočet hodnoty rizika a v popisu samotného vzorce a v neposlední řadě též nesprávné zohlednění varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika (zejm. došlo nejen k úpravě hodnoty hrozby, ale na některých místech též k úpravě hodnoty zranitelnosti).“*. NÚKIB dále uvádí, že předložené materiály pak prezentují postupy hodnocení rizik jak podle pravidel normy ISO 27001, tak podle pravidel obsažených v ZKB a VKB a není tak zřejmé, *„zda a z jakého důvodu zadavatel provádí či hodlá provádět dvojí hodnocení rizik. Žádné z těchto hodnocení však samo o sobě ani v souhrnu nevyhovuje kompletním požadavkům ZKB a VKB.“*.

Postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření je tedy z pohledu NÚKIB *„nedostatečně zdokumentován a je obecně (pro nezainteresovanou osobu) neopakovatelný a zmatečný. Stejně tak je zmatečný i samotný způsob zpracování varování NÚKIB ze dne 17. 12. 2018 do procesu hodnocení rizik.“ Z výše uvedených důvodů pak postup zadavatele nelze označit za souladný se ZKB a VKB.“*.

Ohledně hodnocení souladnosti postupu zadavatele s pravidly obsaženými v normě ISO 27001, NÚKIB uvádí, že *„to obecně není v kompetenci NÚKIB. Ačkoli VKB z uvedené normy v podstatné části vychází (a NÚKIB tedy v mnoha případech při hodnocení zákonnosti postupu povinných osob s obsahem norem řady ISO 27000 pracuje), stále existují určité odlišnosti (…). NÚKIB je pak pověřen dozorováním dodržování ZKB a VKB, nikoli norem řady ISO 27000 (...).“*.

NÚKIB dále uvádí, že nevylučuje, *„že pokud by zadavatel provedl hodnocení rizik řádně podle všech pravidel obsažených ve VKB a vyvaroval se výše uvedeným pochybením, výsledek hodnocení rizik by byl shodný a rozporované bezpečnostní opatření by bylo pro snížení identifikovaných rizik možné i nadále považovat za jediné akceptovatelné (…)“* a, jak již NÚKIB uvedl výše, *„zadavatel sice nesprávně zohlednil varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika, současně však výslovně zmínil, avšak dále nehodnotil rizika, která by mohla být z pohledu NÚKIB relevantní a u nichž by hodnota rizika pravděpodobně také překročila hranici pro akceptaci rizika (…)“* a dále NÚKIB poznamenává, že *„[s]tejně tak nelze vyloučit, že zadavatelův postup ve výsledku*

vyhovuje požadavkům normy ISO 27001. (…) je však třeba uzavřít, že výběr bezpečnostního opatření se nezakládá na hodnocení rizik provedeném zcela v souladu s požadavky ZKB a VKB.“.

Právní posouzení

93. Úřad nejprve v obecné rovině uvádí, že řádné stanovení zadávacích podmínek je jednou ze základních povinností zadavatele v rámci zadávacího řízení a má výrazný dopad na další průběh zadávacího řízení, neboť potenciální dodavatelé se na základě zadávacích podmínek rozhodují, zda se budou o předmětnou veřejnou zakázku ucházet. Zadávací podmínky by tak měly představovat konkrétní vyjádření jednotlivých požadavků zadavatele, jež je formálně zachyceno v zadávací dokumentaci. Jedná se o podmínky, jež by zadavatel měl stanovit v souladu a v mezích příslušných ustanovení zákona, zejména pak základních zásad dle ustanovení § 6 zákona, a měl by věnovat dostatečnou pozornost jejich kvalitnímu zpracování.

94. Úřad dále uvádí, že je nutné vždy vycházet ze smyslu a účelu právní úpravy zadávání veřejných zakázek, kdy primárním cílem zákona je zajištění nejvyšší možné transparentnosti procesu zadávání veřejných zakázek, co možná nejotevřenější soutěže a férového prostředí jako předpokladu pro hospodárné vynakládání veřejných prostředků. Tím, že mezi jednotlivými dodavateli probíhá hospodářská soutěž, jsou tito nuceni nabídnout zadavateli co možná nejvýhodnější podmínky nabízeného plnění. Předpokladem pro existenci hospodářské soutěže mezi dodavateli je pak konkurenční prostředí, ve kterém mají potenciální dodavatelé rovné podmínky, a hospodářská soutěž není ze strany zadavatele deformována.

95. S odkazem na ustanovení § 36 odst. 1 zákona pak Úřad uvádí, že zadávací podmínky musí být nastaveny tak, aby vůči všem potenciálním dodavatelům působily nediskriminačně, tj. v souladu se zásadou zákazu diskriminace stanovenou v ustanovení § 6 odst. 2 zákona, přičemž z tohoto základního pravidla vyplývá, že zadávací podmínky nesmí určitému okruhu dodavatelů či přímo jednomu dodavateli bezdůvodně přímo či nepřímo zajišťovat jakoukoli konkurenční výhodu. Zároveň zadavatel nesmí tyto podmínky stanovit tak, aby v jejich důsledku docházelo bezdůvodně k vytváření překážek hospodářské soutěže mezi jednotlivými potenciálními dodavateli. Je nepochybné, že po zadavateli nelze reálně požadovat, aby stanovené zadávací podmínky měly na všechny dodavatele stejný dopad a nevytvářely tak určitou nerovnováhu mezi dodavateli. Přesto případné omezení musí být vždy odůvodnitelné oprávněnými potřebami zadavatele a je to právě zadavatel, kdo musí unést důkazní břemeno, že se skutečně nejedná o bezdůvodnou překážku hospodářské soutěže mezi jednotlivými potenciálními dodavateli předmětu plnění veřejné zakázky. Případným porušením se tak zadavatel nedopouští pouze porušení ustanovení § 36 odst. 1 zákona, ale také porušení základních zásad zakotvených v ustanovení § 6 zákona.

96. K již výše zmíněné povinnosti zadavatele dodržovat při svém postupu zásadu zákazu diskriminace pak Úřad odkazuje např. na rozsudek Nejvyššího správního soudu sp. zn. 5 Afs 131/2007 ze dne 12. 5. 2008, v němž citovaný soud mj. uvedl, že: *„Porušení zásady nediskriminace zadávacího řízení by nesporně nastalo, pokud by zadavatel v téže situaci a v týchž otázkách přistupoval k některým uchazečům o veřejnou zakázku procedurálně nebo obsahově jinak než ke zbylým, popř. pokud by v důsledku zadavatelova postupu bylo*

některým uchazečům objektivně znemožněno nebo ztíženo ucházet se o veřejnou zakázku za podmínek, za nichž se o ni mohou ucházet jiní uchazeči.“. V rozsudku č. j. 1 Afs 20/2008-152 ze dne 5. 6. 2008 pak Nejvyšší správní soud konstatoval, že *„(…) toto ustanovení totiž v prvé řadě směřuje k cíli samotného zákona o veřejných zakázkách, kterým je zajištění hospodárnosti, efektivnosti a účelnosti nakládání s veřejnými prostředky. Zákon tohoto cíle dosahuje především vytvářením podmínek pro to, aby smlouvy, jejichž plnění je hrazeno z veřejných prostředků, byly zadavateli uzavírány při zajištění hospodářské soutěže a konkurenčního prostředí mezi dodavateli (…).“*. Pro úplnost Úřad dodává, že přestože se závěry soudu učiněné ve výše uvedených rozsudcích vztahují k zákonu č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, lze závěry soudu ohledně smyslu zásady zákazu diskriminace zcela jistě aplikovat rovněž ve vztahu k zákonu, neboť princip zásady zákazu diskriminace zůstal i v souvislosti s nynější právní úpravou zachován, tedy nezměněn.

97. V šetřeném případě je mezi účastníky správního řízení mj. sporu o tom, zda zadávací podmínka uvedená v odst. 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace spočívající v tom, že technické a programové prostředky dotčených společností uvedených ve varování NÚKIB nebudou akceptovány a tudíž jsou vyloučeny z předmětného zadávacího řízení, je stanovena v souladu se zákonem. Navrhovatel namítá, že sporná zadávací podmínka vytváří bezdůvodné překážky hospodářské soutěže ve smyslu ustanovení § 36 odst. 1 zákona a je stanovena v rozporu se základními zásadami zakotvenými v § 6 zákona (blíže viz bod 9. a následující odůvodnění tohoto rozhodnutí).

98. Úřad se tak pro posouzení otázky, zda zadavatel stanovil spornou podmínku v rozporu se zákonem, konkrétně s ustanovením § 36 odst. 1 zákona a ustanovením § 6 zákona, zabýval nejprve tím, zda spornou podmínku zadavatel stanovil v souladu se ZKB a VKB a v míře nezbytně nutné, ve smyslu § 4 odst. 4 ZKB, přičemž na tomto místě předesílá, že své posouzení zakládá zejména na stanovisku, které mu na žádost ze dne 17. 10. 2019 poskytl příslušný ústřední orgán státní správy pro oblast kybernetické bezpečnosti, tj. NÚKIB (blíže viz bod 92. odůvodnění tohoto rozhodnutí).

99. Ve stanovisku NÚKIB ze dne 25. 11. 2019 NÚKIB v prvé řadě uvádí, že po prostudování rozhodných dokumentů (blíže viz bod 42. odůvodnění tohoto rozhodnutí) a dalších rozhodných dokumentů (blíže viz bod 92. odůvodnění tohoto rozhodnutí) předložených zadavatelem, v současné době neeviduje zadavatele jako povinnou osobu podle § 3 ZKB a do dnešního dne *„nevydal žádné rozhodnutí nebo opatření obecné povahy, kterým by zadavatele určil povinnou osobou podle § 3 ZKB, a žádné řízení o určení v současné době nevede. (…) zadavatel do dnešního dne neinformoval NÚKIB o tom, že by byl některou z povinných osob, u kterých dochází k tzv. samourčení (…). NÚKIB nadto ani nedisponuje informacemi, na základě kterých by získal důvodné podezření, že zadavatel je povinnou osobou podle § 3 ZKB a v rozporu se zákonem své kontaktní údaje nenahlásil.“*. V této souvislosti NÚKIB dále uvádí, že ani Statutární město Ústí nad Labem, pro které zadavatel, tak jak je mj. uvedeno v odst. 5.3. zadávací dokumentace, v rámci svých činností technicky zajišťuje chod sítě a provoz informačních systémů *„není povinnou osobou podle § 3 ZKB (ani na základě rozhodnutí NÚKIB, ani na základě samourčení)“* a podle vyjádření NÚKIB *„[z]adavatel tedy v současné době není ani provozovatelem informačního nebo*

komunikačního systému povinné osoby ve smyslu § 2 písm. g) ZKB“ a dle NÚKIB ani významným dodavatelem ve smyslu § 2 písm. n) VKB.

100. V této souvislosti NÚKIB uzavírá, *„že pokud není zadavatel povinnou osobou podle ZKB, nelze u něj dovodit ani povinnost postupovat podle pravidel obsažených v ZKB.“*, což však podle vyjádření NÚKIB *„neznamená, že by zadavatel nemohl aplikovat ustanovení ZKB a VKB ve svých strukturách dobrovolně, např. z důvodu, že to po něm požadují jeho smluvní partneři nebo jeho zřizovatel, nebo z důvodu, že zadavatel usiluje o získání certifikace ISO 27000 (…)“*, neboť, jak NÚKIB dále uvádí, zadavatel na str. 4 dokumentu „Dílčí riziková analýza zaměřená na diskové pole a aktivní síťové prvky v core vrstvě“ uvádí, že *»„[s]polečnost Metropolnet zajišťuje přístup přes síť MVČR ke kritické infrastruktuře státu z pohledu zákona o kybernetické bezpečnosti (KIVS = komunikační infrastruktura veřejné správy, CMS = centrální místo služeb). Tudíž je nutné, aby požadavky kladené na Kritickou infrastrukturu MV splňovala i firma Metropolnet, tj. prakticky naplňovala požadavky Kybernetického zákona“.*«, z čehož dle NÚKIB zadavatel dovozuje svou povinnost zajišťovat bezpečnost informací podle ZKB, neboť přistupuje do systémů, které musejí požadavky ZKB splňovat.

101. Zadavatel se pak k této skutečnosti vyjádřil ve svém nedatovaném vyjádření k podkladům rozhodnutí, kdy mj. uvedl, že *„dobrovolně přistoupil k aplikaci vybraných povinností dle ZKB/VKB“*.“

102. Úřad na tomto místě považuje za nutné s ohledem na výše uvedené zdůraznit, že nijak nepolemizuje s argumentací zadavatele, že k aplikaci ustanovení ZKB a VKB ve svých strukturách přistoupil dobrovolně, nicméně dle názoru Úřadu je tato argumentace ve vztahu k šetřenému případu irelevantní. Z hlediska posouzení, zda zadavatel stanovil spornou podmínku v souladu se zákonem, je rozhodné stanovisko NÚKIB, ze kterého bude vyplývat, zda zadavatel spornou podmínku stanovil v souladu s příslušnými ustanoveními ZKB a VKB či nikoliv.

103. Zadavatel ve svém vyjádření k návrhu ze dne 23. 9. 2019 uvádí a je přesvědčen, že *„svůj postup považuje za zákonný, důvodný, aplikující povinnosti plynoucí ze zákona o kybernetické bezpečnosti a jeho prováděcího předpisu, jakož i z varování NÚKIB, což založilo oprávněný důvod k vyloučení předmětných technologií v zadávacím řízení, a tedy v konečném důsledku stěžovatele. V důsledku uvedeného zadavatel postupoval tak, že neporušil ust. § 36 odst. 1 ZZVZ, ani zásady, na kterých ZZVZ spočívá (§ 6 ZZVZ).“*.

104. Ohledně samotného posouzení souladnosti postupu zadavatele při tvorbě analýzy rizik s ustanoveními ZKB a VKB, NÚKIB ve svém stanovisku v prvé řadě uvádí, že *„obsah analýzy rizik a způsob jejího provedení je třeba posuzovat i v kontextu předcházejících a navazujících kroků zadavatele tvořících v souhrnu proces řízení rizik. Proces řízení rizik sestává z hodnocení rizik (jehož součástí je identifikace, analýza a vyhodnocení rizik), výběru a zavedení opatření ke zvládání rizik, sdílení informací o riziku a sledování a přezkoumání rizik [srov. § 2 písm. i) VKB]. Výběr konkrétního bezpečnostního opatření, jehož implementace sníží hodnotu rizika na akceptovatelnou úroveň, pak musí být založen nikoli pouze na samotné analýze rizik (jejímž výsledkem je striktně vzato pouze stanovení hodnoty rizika), nýbrž i na navazujícím vyhodnocení rizik (tedy určení, zda je riziko akceptovatelné či nikoli) a zvážení v úvahu přicházejících bezpečnostních opatření. (…) Pro posouzení správnosti postupu povinné osoby při tvorbě analýzy rizik je krom jiného nezbytné i posouzení toho, zda celý proces hodnocení*

rizik, do něhož tvorba analýzy rizik spadá a od jehož zbylých součástí je funkčně neoddělitelná, byl proveden v souladu s metodikou k tomu vyhotovenou [srov. § 5 odst. 1 písm. a) VKB].“.

105. NÚKIB dále uvádí, že *„[p]o prostudování poskytnutých dokumentů NÚKIB konstatuje, že hodnocení rizik zadavatelem, jak bylo v předložených dokumentech prezentováno, ve vztahu ke konkrétní veřejné zakázce neodpovídá požadavkům obsaženým v ZKB a VKB.“*. Jako nedostatečnou NÚKIB shledává zejména *„identifikaci primárních a podpůrných aktiv a vazeb mezi nimi, výběr konkrétních podpůrných aktiv, na základě jejichž hodnocení došlo k zákazu použití prostředků dotčených obchodních společností v zadávacím řízení, dále lze identifikovat určitou zmatečnost a nejednotnost v popisu stupnic pro hodnocení jednotlivých proměnných vzorce pro výpočet hodnoty rizika a v popisu samotného vzorce a v neposlední řadě též nesprávné zohlednění varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika (zejm. došlo nejen k úpravě hodnoty hrozby, ale na některých místech též k úpravě hodnoty zranitelnosti).“*. NÚKIB dále uvádí, že předložené materiály pak prezentují postupy hodnocení rizik jak podle pravidel normy ISO 27001, tak podle pravidel obsažených v ZKB a VKB a není tak zřejmé, *„zda a z jakého důvodu zadavatel provádí či hodlá provádět dvojí hodnocení rizik. Žádné z těchto hodnocení však samo o sobě ani v souhrnu nevyhovuje kompletním požadavkům ZKB a VKB.“*.

106. Postup zadavatele při hodnocení rizik a při navazujícím výběru bezpečnostního opatření je tedy z pohledu NÚKIB *„nedostatečně zdokumentován a je obecně (pro nezainteresovanou osobu) neopakovatelný a zmatečný. Stejně tak je zmatečný i samotný způsob zpracování varování NÚKIB ze dne 17. 12. 2018 do procesu hodnocení rizik. Z výše uvedených důvodů pak postup zadavatele nelze označit za souladný se ZKB a VKB.“*.

107. Ohledně hodnocení souladnosti postupu zadavatele s pravidly obsaženými v normě ISO 27001, NÚKIB uvádí, že *„to obecně není v kompetenci NÚKIB. Ačkoli VKB z uvedené normy v podstatné části vychází (a NÚKIB tedy v mnoha případech při hodnocení zákonnosti postupu povinných osob s obsahem norem řady 27000 pracuje), stále existují určité odlišnosti (…). NÚKIB je pak pověřen dozorováním dodržování ZKB a VKB, nikoli norem řady ISO 27000 (...).“*.

108. V závěru svého stanoviska NÚKIB uvádí, že nevylučuje, *„že pokud by zadavatel provedl hodnocení rizik řádně podle všech pravidel obsažených ve VKB a vyvaroval se výše uvedeným pochybením, výsledek hodnocení rizik by byl shodný a rozporované bezpečnostní opatření by bylo pro snížení identifikovaných rizik možné i nadále považovat za jediné akceptovatelné“* a, jak již NÚKIB uvedl výše, *„zadavatel sice nesprávně zohlednil varování NÚKIB ze dne 17. 12. 2018 při stanovení hodnot jednotlivých proměnných vzorce pro výpočet rizika, současně však výslovně zmínil, avšak dále nehodnotil rizika, která by mohla být z pohledu NÚKIB relevantní a u nichž by hodnota rizika pravděpodobně také překročila hranici pro akceptaci rizika (…)“* a dále NÚKIB poznamenává, *že „[s]tejně tak nelze vyloučit, že zadavatelův postup ve výsledku vyhovuje požadavkům normy ISO 27001. (…) je však třeba uzavřít, že výběr bezpečnostního opatření se nezakládá na hodnocení rizik provedeném zcela v souladu s požadavky ZKB a VKB.“*.

109. Lze tedy uzavřít, že pokud ze stanoviska NÚKIB jednoznačně vyplývá, že postup zadavatele není souladný s požadavky ZKB a VKB, neexistovaly na straně zadavatele žádné relevantní

důvody pro vyloučení dotčených výrobků ze zadávacího řízení a tím pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu dotčené výrobky. Sporná podmínka je tak stanovena v rozporu s ustanovením § 36 odst. 1 zákona a představuje nepovolenou diskriminaci navrhovatele a omezení hospodářské soutěže ve vztahu k dodavatelům, kteří na trhu nabízejí dotčené výrobky. Úřad v této souvislosti zdůrazňuje, že závěr vyplývající ze stanoviska NÚKIB (tedy že postup zadavatele není souladný s požadavky ZKB a VKB) mimochodem nepopírá ani sám zadavatel, když ve svém vyjádření k podkladům rozhodnutí mj. uvedl, že *„[z]adavatel tak sice nepostupoval jednoznačně v souladu s požadavky ZKB/VKB (na úrovni metodické), ale podstatná rizika identifikoval a svým postupem je snížil na akceptovatelnou úroveň.“*.

110. Pro úplnost Úřad ohledně skutečnosti uvedené ve stanovisku NÚKIB, že *„[s]tejně tak nelze vyloučit, že zadavatelův postup ve výsledku vyhovuje požadavkům normy ISO 27001. (…).“,* akcentuje, že se zadavatel ve vztahu k vyloučení dotčených výrobků ze zadávacího řízení v zadávací dokumentaci na normu ISO 27001 nijak neodvolává, natož, aby vyhověním požadavkům normy ISO 27001 odůvodňoval vyloučení dotčených výrobků ze zadávacího řízení. Zadavatel se, jak je jasně patrno z článku 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace, v souvislosti s vyloučením dotčených výrobků ze zadávacího řízení odvolává pouze na „Varování č. j. 3012/2018-NÚKIB-E/110“ ze dne 17. 12. 2018 a „Metodiku k varování ze dne 17. prosince 2018“ ze dne 4. 1. 2019 vydanými NÚKIB. Úřad má tudíž za to, že pokud, jak již uvedl výše, ze stanoviska NÚKIB jednoznačně vyplývá, že postup zadavatele není souladný s požadavky ZKB a VKB, neexistovaly na straně zadavatele žádné relevantní důvody pro vyloučení dotčených výrobků ze zadávacího řízení a tím pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu dotčené výrobky, byl v posuzované věci zjištěn skutkový stav tak, aby o něm nebyly důvodné pochybnosti. Úřad nad rámec uvedeného doplňuje, že skutečnost, kdy zadavatel ve svém vyjádření k podkladům pro rozhodnutí uvedl, že se „chystá“ k certifikaci normy ISO 27001, nemůže odůvodnit tak zásadní omezení hospodářské soutěže, jakým je dle Úřadu výše uvedený postup zadavatele (tj. vyloučení dotčených výrobků ze zadávacího řízení a tím pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu dotčené výrobky), neboť v případě, že by tomu tak bylo, považoval by Úřad takový postup zadavatele za nepřiměřený.

111. Na základě výše uvedených skutečností Úřad konstatuje, že zadavatel stanovil zadávací podmínky v zadávacím řízení na předmětnou veřejnou zakázku v rozporu s ustanovením § 36 odst. 1 zákona ve spojení se zásadou zákazu diskriminace zakotvenou v ustanovení § 6 odst. 2 zákona tím, že stanovil zadávací podmínky tak, že vytvářely bezdůvodné překážky hospodářské soutěže, když v článku 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace, mj. stanovil, že vylučuje technické a programové prostředky dotčených společností z předmětného zadávacího řízení, a to s odvoláním na „Varování č. j. 3012/2018-NÚKIB-E/110“ ze dne 17. 12. 2018 a „Metodiku k varování ze dne 17. prosince 2018“ ze dne 4. 1. 2019 vydanými NÚKIB, ačkoliv neexistovaly relevantní důvody na straně zadavatele pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu výše uvedené technické a programové prostředky, a zadavatel tak nedodržel zásadu zákazu diskriminace ve vztahu k navrhovateli.

112. S ohledem na tuto skutečnost rozhodl Úřad tak, jak je uvedeno ve výroku I. tohoto rozhodnutí.

K dalším v návrhu namítaným skutečnostem

113. Úřad na tomto místě v prvé řadě konstatuje, že s ohledem na skutečnost, že z předložené dokumentace o zadávacím řízení a stanoviska NÚKIB ze dne 25. 11. 2019 vyvodil, že zadavatel stanovil zadávací podmínky v rozporu se zákonem (blíže viz odůvodnění k výroku I. tohoto rozhodnutí), v důsledku čehož Úřad zrušil zadávací řízení (v podrobnostech viz dále), považuje za nadbytečné zabývat se ostatními argumenty navrhovatele. Úřad má za to, že šetření dalších skutečností uvedených v návrhu by nemohlo mít vliv na výsledek rozhodnutí Úřadu v předmětném případě, tj. na to, že zadavatel stanovil zadávací podmínky v rozporu se zákonem, důsledkem čehož je přijetí nápravného opatření dle § 263 odst. 3 zákona - zrušení zadávacího řízení. Úřad tak postupuje v souladu s ustálenou rozhodovací praxí, dle níž zkoumání dalších důvodů pro uložení nápravného opatření je nadbytečné, existuje-li alespoň jeden oprávněný důvod. Takový postup v rámci přezkumu je nejen v souladu s rozhodovací praxí Úřadu a správních soudů, ale je zejména v souladu se zásadou procesní ekonomie stanovenou v § 6 odst. 2 správního řádu. Je neúčelné, aby se Úřad věcně zabýval všemi důvody pro uložení nápravného opatření a k prokázání či vyvrácení jejich existence prováděl rozsáhlé dokazování, jež neúměrně zatíží účastníky řízení i Úřad a případně též nedůvodně pozdrží průběh zadávacího řízení. Pokud tedy Úřad dospěje k závěru, že alespoň jeden důvod pro uložení nápravného opatření existoval, je zkoumání existence dalších důvodů, jež by případně vedly k přijetí téhož nápravného opatření, nadbytečné.

K výroku II. tohoto rozhodnutí

114. Podle § 263 odst. 3 zákona stanoví-li zadavatel zadávací podmínky v rozporu s tímto zákonem, Úřad uloží nápravné opatření spočívající ve zrušení zadávacího řízení.

115. Úřad konstatuje, že zadavatel stanovil zadávací podmínky v zadávacím řízení na předmětnou veřejnou zakázku v rozporu s ustanovením § 36 odst. 1 zákona ve spojení se zásadou zákazu diskriminace zakotvenou v ustanovení § 6 odst. 2 zákona tím, že stanovil zadávací podmínky tak, že vytvářely bezdůvodné překážky hospodářské soutěže, když v článku 5.3. „Vyloučení dodávek konkrétních technických a programových prostředků“ zadávací dokumentace, mj. stanovil, že vylučuje technické a programové prostředky dotčených společností z předmětného zadávacího řízení, a to s odvoláním na „Varování č. j. 3012/2018-NÚKIB-E/110“ ze dne 17. 12. 2018 a „Metodiku k varování ze dne 17. prosince 2018“ ze dne 4. 1. 2019 vydanými Národním úřadem pro kybernetickou a informační bezpečnost, ačkoliv neexistovaly relevantní důvody na straně zadavatele pro omezení hospodářské soutěže ve vztahu k dodavatelům nabízejícím na trhu výše uvedené technické a programové prostředky, a zadavatel tak nedodržel zásadu zákazu diskriminace ve vztahu k navrhovateli.

116. Úřad proto s ohledem na výše uvedené rozhodl o zrušení zadávacího řízení, jak je uvedeno ve výroku II. tohoto rozhodnutí.

K výroku III. tohoto rozhodnutí

117. Podle § 263 odst. 8 zákona ukládá-li Úřad nápravné opatření s výjimkou zákazu plnění smlouvy, zakáže zároveň zadavateli až do pravomocného skončení řízení uzavřít v zadávacím řízení smlouvu; rozklad proti tomuto výroku nemá odkladný účinek.

118. Výše citované ustanovení formuluje obligatorní součást rozhodnutí Úřadu o uložení nápravného opatření (s výjimkou zákazu plnění smlouvy) rovněž výrok o tom, že zadavatel až do pravomocného skončení správního řízení nesmí uzavřít smlouvu v zadávacím řízení, přičemž tento výrok je účinný dnem vydání rozhodnutí, a tedy je účinný i u nepravomocného rozhodnutí. Tento zákaz uzavřít smlouvu se ukládá z důvodu, aby se zadavatel nemohl vyhnout splnění uloženého nápravného opatření uzavřením smlouvy ještě před nabytím právní moci rozhodnutí.

119. Vzhledem k tomu, že Úřad tímto rozhodnutím ve výroku II. uložil nápravné opatření spočívající ve zrušení předmětného zadávacího řízení, zakázal zároveň ve výroku III. tohoto rozhodnutí zadavateli až do pravomocného skončení tohoto správního řízení uzavřít v předmětném zadávacím řízení smlouvu na veřejnou zakázku.

K výroku IV. tohoto rozhodnutí

120. Podle § 266 odst. 1 zákona je součástí rozhodnutí Úřadu, kterým se ukládá nápravné opatření nebo zákaz plnění smlouvy, též rozhodnutí o povinnosti zadavatele uhradit náklady správního řízení. Náklady řízení se platí paušální částkou, kterou stanoví Ministerstvo pro místní rozvoj vyhláškou. Příslušná vyhláška č. 170/2016 Sb., o stanovení paušální částky nákladů řízení o přezkoumání úkonů zadavatele při zadávání veřejných zakázek, stanoví v § 1, že paušální částka nákladů řízení o přezkoumání úkonů zadavatele, kterou je povinen zadavatel uhradit v případě, že Úřad rozhodl o uložení nápravného opatření nebo zákazu plnění smlouvy, činí 30 000 Kč.

121. Vzhledem k tomu, že Úřad tímto rozhodnutím ve výroku II. uložil nápravné opatření spočívající ve zrušení zadávacího řízení na veřejnou zakázku, rozhodl Úřad o uložení povinnosti uhradit náklady řízení, jak je uvedeno ve výroku IV. tohoto rozhodnutí.

122. Náklady řízení jsou splatné do dvou měsíců od nabytí právní moci tohoto rozhodnutí na účet Úřadu pro ochranu hospodářské soutěže zřízený u pobočky České národní banky v Brně číslo 19-24825621/0710, variabilní symbol – 2019000358.

POUČENÍ

Proti tomuto rozhodnutí lze do 15 dnů ode dne jeho doručení podat rozklad k předsedovi Úřadu pro ochranu hospodářské soutěže, a to prostřednictvím Úřadu pro ochranu hospodářské soutěže – sekce veřejných zakázek, třída Kpt. Jaroše 1926/7, Černá Pole, 604 55 Brno. Včas podaný rozklad proti výroku I., II. a IV. tohoto rozhodnutí má odkladný účinek. Rozklad proti výroku III. tohoto rozhodnutí nemá podle § 263 odst. 8 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, odkladný účinek. Rozklad a další podání účastníků učiněná v řízení o rozkladu se podle § 261 odst. 1 písm. b) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, zasílají Úřadu výhradně prostřednictvím datové schránky nebo jako datová zpráva podepsaná uznávaným elektronickým podpisem.

otisk úředního razítka

JUDr. Eva Kubišová
místopředsedkyně

Obdrží

1. Metropolnet, a.s., Mírové náměstí 3097/37, Ústí nad Labem-centrum, 400 01 Ústí nad Labem
2. Huawei Technologies (Czech) s.r.o., Jihlavská 1558/21, Michle, 140 00 Praha 4

Vypraveno dne

viz otisk razítka na poštovní obálce nebo časový údaj na obálce datové zprávy