VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE č. 2

dle § 98 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek ve znění pozdějších předpisů
(dále jen také „ZZVZ“)

Zadavatel:	Nemocnice Pardubického kraje, a.s.
Sídlo:	Kyjevská 44, 532 03 Pardubice
IČO:	275 20 536
Zastoupený:	MUDr. Tomášem Gottvaldem, MHA, předsedou představenstva Ing. Františkem Lešundákem, místopředsedou představenstva
Název veřejné zakázky:	Rekonstrukce počítačové sítě NPK – zajištění integrity sítě prostřednictvím zavedení jednotného systému páteřních a přístupových přepínačů – 3. kolo
Režim veřejné zakázky:	Nadlimitní
Druh zadávacího řízení:	Otevřené řízení
Druh veřejné zakázky:	Dodávky
Systémové číslo veřejné zakázky:	P20V00000021
Evidenční číslo zakázky ve VVZ:	Z2020-002276

V Pardubicích dne 13. 2 2020

Zadavatel obdržel prostřednictvím datové schránky dne 10. 2. 2020 následující dotaz, na který podává níže uvedené vysvětlení.

Dotaz č. 1:

Naše společnost po prostudování zadávací dokumentace (výše uvedené veřejné zakázky) zjistila, že tato vůbec nezohledňuje rizika, která pojmenoval Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) ve vztahu k technickým nebo programovým prostředkům společností **Huawei Technologies Co., Ltd. a ZTE Corporation**.

Zadavatelem poptávané řešení je určeno pro provozování významných informačních systémů a informačních systémů kritické informační infrastruktury (zejména viz čl. 1.7 a 4.3 zadávací dokumentace). Zadavatel tedy spadá pod dikci zákona č.181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „Zákon o kybernetické bezpečnosti“). Dodané řešení tak nesmí být tedy v rozporu s požadavky (dále jen NÚKIB) pro provoz prvků kritické informační infrastruktury.

Dodané řešení musí proto splňovat všechny související požadavky a nařízení a musí umožňovat Zadavateli řádné plnění povinností podle Zákona o kybernetické bezpečnosti. V souladu s výše uvedeným je Zadavatel povinen dle § 5 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, provádět analýzu rizik a identifikovaná rizika řídit.

Současně je Zadavatel povinen zabývat se všemi hrozbami, které prostřednictvím varování vydává NÚKIB, a zohlednit je v analýze rizik. Zadavatel proto musí při hodnocení rizik (a logicky též při stanovení zadávacích podmínek) přihlédnout též k vydaným **Varování NÚKIB ze dne 17. 12. 2018** a dokumentu NÚKIB „Metodika k varování ze dne 17. prosince 2018“, které reaguje na použití technických a programových prostředků společností Huawei Technologies Co., Ltd. a ZTE Corporation, včetně jejich dceřiných společností.

Jediným možným bezpečnostním opatřením v návaznosti na shora uvedené, kterým lze objektivně snížit hodnotu rizika na akceptovatelnou úroveň, je vyloučení technických a programových prostředků společností Huawei Technologies Co., Ltd. a ZTE Corporation, včetně jejich dceřiných společností, z plnění veřejné zakázky. To však Zadavatel v zadávacích podmínkách neučinil resp. ani se o to jakkoliv nepokusil.

Tato skutečnost je zvlášť alarmující v kontrastu k postupu zřizovatele Zadavatele, kterým je **Pardubický kraj**. Zřizovatel Zadavatele si je zjevně při zadání svých veřejných zakázek rizika vědom a toto riziko důsledně řídí a eliminuje.

K tomu odkazujeme například na zadání veřejné zakázky ***Rozšíření regionální datové sítě Pardubického kraje***, jejímž zadavatelem je Pardubický kraj (číslo ve VVZ Z2020-004193), kde zadávací podmínky obsahují níže uvedené omezení:

*„Z důvodu neakceptovatelné míry rizika je pro všechny části sítě kromě modulu Transportního zakázáno realizovat tyto části technickými nebo programovými prostředky společností **ZTE Corporation a Huawei Technologies Co**. se sídlem v Čínské lidové republice, včetně jejich dceřiných firem.*

Podkladem pro tento zákaz je varování Národního úřadu pro kybernetickou a informační bezpečnost ze dne 17.12.2018, jeho metodika ze dne 4.1.2019 a následná analýza rizik zadavatele s ohledem na kategorii přenášených dat Regionální datovou sítí.“

Obdobné omezení pak při zadání svých veřejných zakázek aplikují také ostatní krajské nemocnice v ČR.

Dovolujeme si proto požádat Zadavatele o:

- **vyjádření, zda shora uvedené riziko spojené s možností aplikace technických a programových prostředků společností Huawei Technologies Co., Ltd. a ZTE Corporation považuje za relevantní.**

- **V případě kladné odpovědi na předchozí dotaz, tzn. neakceptování aplikace technických a programových prostředků (produktů) společností Huawei Technologies Co., Ltd. a ZTE Corporation žádáme o vyjádření, zda Zadavatel upraví zadávací podmínky směrem k vyloučení technických a programových prostředků společností Huawei Technologies Co., Ltd. a ZTE Corporation z plnění předmětné veřejné zakázky Zadavatele pod názvem „Rekonstrukce počítačové sítě NPK – zajištění integrity sítě prostřednictvím zavedení jednotného systému páteřních a přístupových přepínačů – 3. kolo“.**

- **V případě negativní odpovědi na předchozí dotaz, žádáme o vyjádření, z jakého důvodu Zadavatel postupuje při zadání veřejné zakázky dle jiných principů než jeho zřizovatel (Pardubický kraj).**

Závěrem poznamenáváme, že tuto naši žádost nelze vnímat jen jako prosté vymezení se proti výše zmíněným společnostem. Naše společnost zvažuje možnost podání nabídky různých technologií splňující podmínky zadávací dokumentace, a to potenciálně včetně produktů společnosti Huawei Technologies Co., Ltd.

Nicméně s ohledem na aktuální situaci a varování NÚKIB chceme mít úplnou jistotu, zda Zadavatel umožní či neumožní tyto technické a programové prostředky (produkty) uchazečům nabídnout a nevyloučit je na základě varování NÚKIB či jiných prostředků. V návaznosti na odpověď Zadavatele pak budeme koncipovat svoji nabídku. Na každý pád se chceme vyhnout případným budoucím sporům se Zadavatelem resp. zpracování nabídky, která by nakonec byla pro Zadavatele nepřijatelná. Proto žádáme Zadavatele o zcela jednoznačné stanovisko k tomuto dotazu.

Odpověď zadavatele:

Zadavatel se zabývá všemi hrozbami kybernetické bezpečnosti, samozřejmě i těmi, které prostřednictvím varování vydává NÚKIB. Zadavatel má zpracovanou analýzu rizik, která není součástí zadávací dokumentace a ze které vyplývá, že riziko spojené s užíváním technických a programových prostředků (produktů) společností Huawei Technologies Co., Ltd. a ZTE Corporation (které již mimochodem zadavatel ve své síti používá) je akceptovatelné nasazením již existujícího technického opatření eliminujícího zranitelnost(i) aktiva nebo hrozby spojené s používáním aktiva (firewally třetího výrobce). Pardubický kraj poskytuje spojovou síť (Regionální datovou síť Pardubického kraje) svým zřizovaným organizacím, na kterou působí zcela jiné hrozby.

K tomuto je třeba dodat, že zadavatel je samostatně fungujícím subjektem, akciovou společností, kde Pardubický kraj je jediným akcionářem. Nejedná se tedy o vztah, který by zadavatele a Pardubický kraj blíže propojoval, jak tomu může být např. u příspěvkových organizací zřizovaných územními samosprávnými celky. Provoz zadavatele je řízen standardní strukturou akciové společnosti a v rámci této struktury jsou též přijímány příslušná rozhodnutí. Zadavatel k tomuto disponuje vlastními procesními postupy a vlastními analýzami (včetně příslušné analýzy rizik) zaměřenými výhradně na činnost zadavatele a na rizika s výkonem této činnosti spojena. Proto se zřejmě mohou závěry zadavatele a jeho akcionáře v některých aspektech lišit. Závěrem je však nutné uvést, že zadavatel ze své pozice není oprávněn (ani nechce být oprávněn) jakkoliv hodnotit a posuzovat zadávací podmínky, které jsou nastaveny jiným zadavatelem a srovnávat tak dva provozně naprosto odlišné subjekty.

Zadavatel neprovedl změnu ani doplnění zadávací dokumentace, které by vyžadovalo prodloužení lhůty pro podání nabídek.

Oddělení veřejných zakázek
Nemocnice Pardubického kraje, a.s.