SOUBOR VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 3

pro zadání nadlimitní veřejné zakázky na dodávky zadávané v otevřeném řízení dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon“)

s názvem

Kybernetická bezpečnost ICT MĚSTSKÉHO ÚŘADU KRÁLÍKY

Zadavatel poskytuje toto následující vysvětlení zadávací dokumentace vztahující se k výše uvedené zakázce

---

Znění žádosti o vysvětlení ZD č. 1:

Zadavatel v požadavcích na technickou kvalifikaci dle § 79 odst. 2 písm. b) ZZVZ požaduje předložení seznamu významných dodávek, konkrétně: „alespoň 1 zakázka obdobného charakteru spočívající v dodávce a implementaci Monitoringu síťového provozu s úložištěm logů v hodnotě alespoň 500.000,- Kč bez DPH."

Dodavatel upozorňuje, že stanovení minimálního finančního limitu 500.000 Kč bez DPH výhradně pro část plnění „Monitoring síťového provozu s úložištěm logů" považuje za nepřiměřené rozsahu a složitosti předmětu plnění a neodpovídající běžným tržním cenám.

Moderní monitorovací nástroje a řešení pro ukládání logů (syslog servery, SIEM light řešení apod.), které plně dostačují pro infrastrukturu poptávaného rozsahu, se cenově pohybují výrazně níže. Požadavek na referenci v hodnotě půl milionu korun tak fakticky cílí na robustní enterprise řešení, která nejsou pro tento typ zakázky nezbytná.

Tímto požadavkem dochází k nedůvodnému omezení hospodářské soutěže, neboť jsou vyloučeni kvalifikovaní dodavatelé, kteří mají s implementací monitoringu bohaté zkušenosti, ale realizují je pomocí efektivnějších a cenově dostupnějších technologií. Schopnost dodavatele realizovat monitoring nelze měřit pouze vysokou cenou předchozího plnění.

Dodavatel navrhuje, aby zadavatel v zájmu rozšíření okruhu možných dodavatelů a dodržení zásady přiměřenosti tento finanční limit buď zcela vypustil (a požadoval pouze prokázání zkušenosti s dodávkou technologie), nebo jej snížil na úroveň odpovídající tržní realitě pro tento segment (např. 100.000 Kč bez DPH).

Vysvětlení ZD č. 1:

Zadavatel je úřadem s rozšířenou působností a zpracovává mimořádně široké spektrum citlivých údajů občanů – od osobních dat z matrik (narození, úmrtí, manželství) přes údaje z registru obyvatel, řidičů a vozidel až po informace z agend sociálně-právní ochrany dětí, přestupků, živnostenského podnikání či stavebních řízení. Součástí jeho činnosti je také zpracování dat týkajících se majetku města, finančních operací, místních poplatků, elektronické spisové služby a interní i externí komunikace úřadu. Tato data mají vysokou citlivost i hodnotu — jejich zneužití může mít vážné dopady na soukromí občanů, chod města i jeho finanční stabilitu.

Směrnice NIS2, implementovaná novým zákonem o kybernetické bezpečnosti Zákon č. 264/2025 Sb. účinným od 1. 11. 2025, řadí zadavatele mezi regulované subjekty, které musí zavést vhodná a robustní kyberbezpečnostní opatření. Patří sem i schopnost včas detekovat incidenty, chránit zpracovávaná data a splnit přísné požadavky na hlášení bezpečnostních událostí. Monitoring a logování představují zásadní obranné mechanismy a jsou zákonnými předpisy přímo vyžadovány. Z tohoto důvodu zadavatel požaduje robustní enterprise řešení pro část plnění „Monitoring síťového provozu s úložištěm logů".

Pro nasazení tohoto řešení zadavatel zároveň požaduje, aby potenciální dodavatel doložil adekvátní reference, které prokazují jeho praktické zkušenosti s realizací obdobně náročných projektů. Tyto zkušenosti jsou klíčové nejen pro zajištění kybernetické bezpečnosti úřadu, ale také vzhledem k významu celé zakázky a dopadu použitých technologií na chod úřadu a zajištění služeb veřejnosti. Z výše uvedených důvodů jsou požadované reference v ZD zcela adekvátní.

Znění žádosti o vysvětlení ZD č. 2:

Plně jsme se seznámili s vysvětlením zadávací dokumentace č. 1, ve kterém zadavatel trvá na požadavku „čelního krytu serveru včetně LCD displeje“. Dodavatel plně respektuje provozní potřebu zadavatele na „at-the-rack“ diagnostiku nezávislou na síti.

Upozorňujeme však na technologický posun v oblasti enterprise serverů, kde přední výrobci přecházejí na přímé lokální rozhraní (Direct Local Management), a to nejen z důvodů vyšší informační hodnoty, ale především z důvodů kybernetické bezpečnosti.

Dodavatel předkládá následující argumenty pro akceptaci rovnocenného řešení:

Vyšší bezpečnost (Ochrana proti neoprávněnému přístupu): Klasické LCD panely na čele serverů často zobrazují citlivé informace (IP adresy management rozhraní, chybové kódy, verze FW) trvale nebo po pouhém stisku tlačítka, bez nutnosti jakékoliv autentizace. To představuje bezpečnostní riziko (tzv. information disclosure), kdy může jakákoliv osoba s fyzickým přístupem k racku získat údaje o konfiguraci infrastruktury. Moderní řešení (připojení servisního zařízení do dedikovaného portu) vyžaduje aktivní krok a v mnoha implementacích i následnou autentizaci technika v servisní aplikaci. Tím je zajištěno, že diagnostická data vidí pouze oprávněná osoba, nikoliv kdokoliv, kdo se pohybuje v serverovně.

Detailnější diagnostika: Zatímco LCD displej je omezen na několik znaků a kódů, řešení využívající externí displej (tablet/mobil/notebook technika připojený k serveru) nabízí plnohodnotné grafické rozhraní, logy a možnosti konfigurace, které jsou na malém LCD panelu technicky nerealizovatelné.

Tento přístup naplňuje účel požadovaný zadavatelem (okamžitá diagnostika bez sítě), ale realizuje jej bezpečnější a modernější formou. Trváním na striktní konstrukční podmínce „LCD displeje“ by zadavatel nutil dodavatele nabízet technologicky starší a méně bezpečné řešení a diskriminoval by moderní standardy.

Zadavatele se tímto tážeme, zda v souladu s § 89 odst. 6 ZZVZ (použití rovnocenného řešení) bude považovat za splnění technické kvalifikace i takové řešení, které namísto fixního LCD displeje (který může představovat bezpečnostní riziko úniku informací) nabízí funkcionalitu přímého lokálního managementu (např. via Direct Connect USB/Service Port), umožňujícího bezpečné vyčtení diagnostických informací přímo u zařízení.

Vysvětlení ZD č. 2:

Přední LCD displej poskytuje okamžitý vizuální přehled o stavu zařízení přímo v uličce racku, bez nutnosti připojovat kabely, otevírat kryty či vyhledávat kompatibilní software. Řešení založené výhradně na servisním portu je svou povahou transakční, kdežto LCD plní roli fail-safe indikátoru – technik okamžitě vidí, který systém a jakým způsobem hlásí problém.

Z toho důvodu zadavatel setrvává na původním požadavku „čelního krytu serveru včetně LCD displeje“. Navrhované řešení zcela nenaplňuje účel požadavku a nebude považováno za rovnocenné podle § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

V Brně, dne 10. 12. 2025

Deregio Tender, s.r.o.
Ing. Jan Ševčík, jednatel
Zástupce zadavatele