

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE 12

Název sektorové veřejné zakázky:	Smart metering elektroměry – Chammeleon
Identifikační údaje o zadavateli	
Název:	EG.D, a.s.
Sídlo:	Brno – Černá Pole, Lidická 1873/36, 602 00
IČO:	28085400
Druh (předmět) zakázky:	Dodávky
Druh zadávacího řízení:	Užší řízení navazující na systém kvalifikace
Režim zakázky:	Nadlimitní

Společnost EG.D, a.s., v zadávacím řízení zastoupena společností RTS, a. s., jako zadavatel shora uvedené sektorové veřejné zakázky, obdržel níže uvedenou žádost o vysvětlení zadávací dokumentace. Na tuto žádosti poskytuje zadavatel následující odpověď:

Dotaz č. 1

Chápeme správně, že pokud zadavatel neakceptuje výhradu dodavatele proti výzvě zadavatele k plnění, která požaduje dodání zboží do 10 týdnů (tj. výhrada dodavatele spočívá v žádosti o akceptaci delší dodací lhůty než 10 týdnů), má zadavatel možnost nárokovat smluvní pokutu ve výši 0,5 % z ceny nedodaného zboží, za každý den prodlení počínaje prvním dnem po 10. týdnu, maximálně však 100 % z ceny nedodaného zboží?

Prosíme o potvrzení nebo korekci našeho výkladu zadávacích podmínek.

Odpověď č. 1

Ano, pokud nenastanou objektivní důvody, které brání dodávce, viz čl. IV. odst. 16 rámcové dohody.

Dotaz č. 2

Kdy může být doručena první výzva k plnění? Chápeme správně, že první výzva k plnění může být doručena **až po naplnění skladu**, tj. nejdříve 11 týdnů po podepsání smlouvy. **Tudíž nejdřívejší možná dodávka zboží tak může být 21 týdnů od podepsání kontraktu?**

Odpověď č. 2

Zadavatel bude objednávat nejméně v souladu s článkem 2. odstavec 6 Rámcové dohody. Zadavatel má připravený celkový plán instalace elektroměrů v rozpadu na roční hodnoty. Hned po podpisu smlouvy a vždy na začátku roku bude zadavatel řešit s dodavateli forecasty na jednotlivé dodávky.

Dotaz č. 3

Jste si vědomi toho, že 10týdenní dodací lhůta je nereálná, a proto **při podpisu smlouvy musí zadavatel domluvit reálný termín dodání** (s nejistým výsledkem) s vítězem výběrového řízení?

Takový postup staví zadavatele do nevýhodné pozice a nezaručuje, že jedná jako „*řádný hospodář*“. Vzhledem k tomu, že skutečný termín dodání není v rámci výběrového řízení určen, nelze rozlišovat mezi prodejci, kteří dodávají měřidla rychleji, a prodejci, kteří měřidla dodávají pomaleji.

Proto navrhuje, aby zadavatel nastavil realistické podmínky (dosažitelné na trhu), které nebude třeba po podpisu smlouvy znovu vyjednávat nebo nechat dodavatele, aby se sami zavázali k dodací lhůtě v rámci Nabídky a závazná dodací lhůta by měla být stanovena v uzavřené smlouvě.

Tímto způsobem bude mít zadavatel podmínky dodání zboží pod kontrolou. Tj. bez nejistého rizika a kdy získá ty nejlepší možné podmínky (což za aktuálních podmínek výběrového řízení neplatí). To by zaručilo rovné zacházení se všemi dodavateli, a tedy žádné preferenční zacházení s jedním z dodavatelů. **Žádáme zadavatele, aby zvážil úpravu zadávacích podmínek.**

Odpověď č. 3

Zadavatel na svých zadávacích podmínkách trvá. Jak již v přechozích odpovědích vysvětlil, ihned po podpisu smlouvy a vždy na začátku roku bude zadavatel řešit s dodavateli forecasty na jednotlivé dodávky. Zároveň platí čl. IV. odst. 16 rámcové dohody o existenci objektivních důvodů při prodlení dodávek.

Dotaz č. 4

Nejsme si jisti, zda se zadavatel svým přístupem k výběru dodavatele, a to bez jakéhokoli důkazu o kybernetické bezpečnosti může dostatečně vyhnout bezpečnostním hrozbám. **V danou chvíli zadavatel řeší kybernetickou bezpečnost pouhým zákazem finálních výrobků z určitých zemí původu.** To je však velmi zkratkový pohled na danou problematiku. Zadavatel tak dává rovnítko k tomu, že určitá země rovná se bezpečný výrobek a jiná země rovná se nebezpečný výrobek.

Rizika jakéhokoliv výrobku nenese výrobek jako takový nebo země sídla společnosti, ale zcela konkrétní, popsatelné a přezkoumatelné technické a konstrukční vlastnosti, programový kód apod. Tyto skutečnosti je pak nutné zkoumat vždy, a to bez ohledu na zemi sídla společnosti.

Z tohoto důvodu vás žádáme, abyste zvážili a uplatňovali požadavky na důkazy a certifikáty kybernetické bezpečnosti tak, jak je to standardem v oboru a součástí best practices v EU jak zajistit bezpečné výrobky v distribuční síti.

Abychom lépe porozuměli tomu, jak správně formálně prokázat, že dodavatel splňuje vaše potřeby, žádáme vás o zpětnou vazbu na následující dvě otázky.

1. Budete akceptovat certifikát o kybernetické bezpečnosti od nezávislého úřadu se sídlem v EU, např. ENCS (<https://encs.eu/>) ?

2. Pokud certifikát podle otázky č. 1 není dostatečný, jaký je dostatečný důkaz kybernetické bezpečnosti produktu s ohledem na vaše tvrzení ve Vysvětlení zadávací dokumentace č. 9, Informace č. 1? Opravdu je pro EG.D důkaz kybernetické bezpečnosti země původu produktu?

Odpověď č. 4

Jak již bylo uvedeno ve Vysvětlení zadávací dokumentace č. 11, Zadavatel nehodlá předjímat postup po podání nabídek, který se bude úzce odvíjet od obsahu podaných nabídek. Dodavatelé jsou povinni předložit takové dokumenty, aby prokázali splnění zadávacích podmínek, včetně prokázání původu předmětu plnění.

Bezpečnostním hrozbám se nelze zcela vyhnout. Lze se na ně pouze připravit a s patřičnými nástroji a přípravou je včas detekovat. Můžeme omezit vektor útoku (např. supply chain attack, vulnerability management, CTI) a připravovat mitigační a nápravné procesy (hardening, backup, apod.).

Bezpečnostní rizika vnímáme v daleko větších souvislostech, než uvádí tazatel (viz. např. technická specifikace, resp. požadavky na bezpečnost v ní uvedené). Dále lze uvést např. požadavky Zadavatele uvedené v čl. 24 VNP a přílohu těchto nákupních podmínek - Technicko-organizační opatření bezpečnosti informací a ochrany osobních údajů, jako součásti příslušného návrhu Rámcové dohody a Servisní smlouvy. Dodavatel (resp. bezpečnost a důvěryhodnost v rámci dodavatelského řetězce) představuje pouze určitou, byť významnou, část bezpečného prostředí a procesů. Z tohoto důvodu je součástí zadání také požadavek či možnost bezpečnostního testování nabízených produktů.

1.

Certifikáty o kybernetické bezpečnosti od nezávislých úřadů (např. ENCS) budou v rámci dodávky z hlediska posuzování bezpečnosti nabízených produktů vstupem, který Zadavatel zohlední, nicméně dodavatel je povinen splnit v první řadě požadavky tak, jak je v této souvislosti definuje zadávací dokumentace. Nelze paušálně říci, že pokud dodavatel předloží nějaký certifikát o kybernetické bezpečnosti (např. ENCS), lze to považovat za splnění zadávacích podmínek. Zároveň rozsah a předmět testování za účelem získání certifikátu se může na základě požadavků zadavatele testů zásadně lišit.

Pokud pak tazatel uvádí, že „**zadavatel řeší kybernetickou bezpečnost pouhým zákazem finálních výrobků z určitých zemí původu**“, patrně má na mysli požadavek zadavatele uvedený v bodě 4.11 zadávací dokumentace – Analýza rizik. Tento požadavek však jednoznačně navazuje na varování NÚKIB ze dne 30.5.2022 (č.j. 6548/2022-NÚKIB-E/350), když okruh zemí, ze kterých smí pocházet příslušné programové a technické prostředky, je definován tímto varováním. Zadavatel je pak povinen toto varování, a tím pádem i seznam zemí pro původ prostředků, respektovat.

2.

Za dostatečné bude zadavatel považovat splnění a doložení všech bezpečnostních požadavků vyplývajících ze zadávací dokumentace. Dále splnění požadavků s ohledem na analýzu rizik ve smyslu varování NÚKIB ze dne 30.5.2022, které zadavatel musí zohlednit ve výběrovém řízení. To vše doplněné (ověřené) nezávislými testy všech požadovaných bezpečnostních parametrů v dostatečné a odpovídající míře podrobnosti (nevylučuje ENCS).

Zadavatel také obecně odkazuje na Vysvětlení zadávací dokumentace č. 6, 9, 10 a 11, které se k dotazu tazatele vztahují.

Dotaz č. 5

Chápeme správně, že technické a programové prostředky, které mohou ovlivnit bezpečnost dle Vysvětlení zadávací dokumentace č. 9, Informace č. 1, jsou jmenovitě: **procesor, paměť a firmware?**

Pokud jde ještě o další komponenty, které budou posuzovány dle výše uvedené Informace, prosíme o taxativní definici těchto technických a programových prostředků.

Aktuálně považujeme požadavek zadavatele za nejasný a může být vysvětlen mnoha způsoby. Zadávací podmínky jsou tak nejednoznačné a vysvětlitelné různými způsoby.

Pokud rozhodnutí o tom, co jsou "technické a programové prostředky" necháte na dodavateli, **prosíme o potvrzení této skutečnosti.**

Závěrem si dovoluujeme požádat o prodloužení lhůty pro podání nabídek, a to o celou původní lhůtu. Důvodem je značná nejasnost a netransparentnost zadávacích podmínek. Věříme, že sám zadavatel má zájem na řádném průběhu zadávacího řízení a k tomu je nutné, aby zadávací podmínky byly zcela jednoznačné a transparentní.

Odpověď č. 5

Jak uvedl zadavatel ve vysvětlení č. 9 zadávací dokumentace ze dne 1. 7. 2022 – na základě varování NÚKIB ze dne 30.5.2022 (č.j. 6548/2022-NÚKIB-E/350), výsledků analýzy rizik a ve spojitosti s povinností uvedenou v § 4 odst. 4 zákona o kybernetické bezpečnosti nelze při realizaci této veřejné zakázky použít takové technické nebo programové prostředky, které mohou ovlivnit bezpečnost (důvěrnost, integritu nebo dostupnost), zejména:

- bezpečnost dat a komponent umožňujících požadovanou úroveň přímého měření typu B, C1, C2 nebo C3 (např. ovlivnění dat z měření a odeslání chybných dat do centrály), nebo
- bezpečnost měření a řízení elektrické energie ve vztahu ke koncovým zákazníkům (např. neoprávněná manipulace s odpojovačem),

a které pocházejí ze států mimo EU, EHP, OECD či NATO.

Ve vztahu k takto relevantním komponentům bude zadavatel posuzovat jejich původ.

Zadavatel také obecně odkazuje na Vysvětlení zadávací dokumentace č. 6, 9, 10 a 11, které se k dotazu tazatele vztahují.

Informace č. 1

Zadavatel rozhodl o prodloužení lhůty pro podání takto:

Lhůta pro podání nabídek končí dne **12. 8. 2022 v 10.00 hod.**