

Zadavatel: Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví
Sídlo: Roškotova 1225/1, 140 00 Praha 4
IČ: 47114321
Veřejná zakázka: „AntiDDos“
Ev. č. zadavatele: 26_VERZAK_0031

V Praze dne, dle elektronického podpisu

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 2 A PRODLOUŽENÍ LHŮTY

I. ODPOVĚDI NA DOTAZY

Výše uvedený zadavatel obdržel ve dnech 4. 5. 2026 a 5. 5. 2026 následující dotazy k nadepsané veřejné zakázce, na které níže poskytuje své odpovědi.

Dotaz č. 3

Zadavatel v čl. VI odst. 6 návrhu smlouvy stanoví povinnost poskytovatele uhradit objednateli jakoukoli veřejnoprávní sankci nebo povinnost plnění uloženou objednateli, a to i v případě nezaviněného jednání poskytovatele, navýšenou o smluvní pokutu ve výši 1 %. Dodavatel má za to, že takto formulované ujednání je nepřiměřené a nepředvídatelné, neboť nevyžaduje porušení konkrétní smluvní či zákonné povinnosti na straně poskytovatele. Poskytovatel nemá možnost předem odhadnout okruh veřejnoprávních povinností objednatele ani potenciální výši sankcí, ani ovlivnit procesní postup objednatele v případném sankčním řízení. Ujednání současně přenáší na poskytovatele odpovědnost za regulatorní rizika objednatele a může vytvářet motivační asymetrii, kdy objednatel nenese plné důsledky vlastního postupu. Dodavatel proto žádá úpravu uvedeného ustanovení tak, aby se vztahovalo výlučně na případy zaviněného porušení konkrétních povinností poskytovatele.

Odpověď na dotaz č. 3

Zadavatel trvá na znění smlouvy.

Ustanovení čl. VI odst. 6 dopadá výlučně na případy, kdy bude veřejnoprávní sankce či povinnost plnění uložena zadavateli (objednateli) v příčinné souvislosti s jednáním či opomenutím poskytovatele při plnění této smlouvy. Nejedná se o přenos obecného regulatorního rizika objednatele na poskytovatele.

Zadavatel současně uvádí, že odpovědnost poskytovatele se neuplatní v případech, kdy sankce vznikne výlučně z důvodů na straně objednatele nebo třetích osob, které poskytovatel nemohl ovlivnit.

Zadavatel se předmětným ustanovením chrání před jednáním poskytovatele, následkem kterého může dojít k situaci, že v důsledku tohoto jednání bude objednatel vystaven veřejnoprávní sankci či povinnosti plnění ve prospěch třetí osoby. Takové jednání poskytovatele v sobě totiž nutně nemusí zahrnovat složku zavinění (úmysl, nedbalost). Citované ustanovení smlouvy je tak prevencí případných sporů ohledně existence zavinění poskytovatele, když odpovědnost poskytovatele je v takovém případě stavěna do roviny tzv. objektivní odpovědnosti podnikatele (tzn. odpovědnosti „za výsledek“). Fakticky se může jednat např. o případy nešťastné náhody (např. únik citlivých dat chybou aplikace), něčí nepřičetnosti na straně poskytovatele, omylu atd., v důsledku kterých může dojít k takovému porušení smlouvy, že za takovéto porušení může být sankcionován objednatel. V žádném případě uvedené neznamená, že by byl poskytovatel objednatelům jakkoli sankcionován v případech, kdy by došlo k jednoznačnému zavinění/zjevných pochybeních ze strany objednatele.

Zadavatel nepřipouští úpravu ustanovení.

Dotaz č. 4

V čl. 6 odst. 7 závazného návrhu smlouvy je uvedeno právo objednatele požadovat vedle smluvní sankce rovněž náhradu škody v plné výši. Dodavatel má za to, že takto nastavená kombinace odpovědnostních a sankčních mechanismů neodpovídá povaze poskytovaných anti-DDoS služeb ani

obvyklé tržní praxi v oblasti kybernetické bezpečnosti. Anti-DDoS služby jsou poskytovány na základě definovaných SLA, která reflektují reálně dosažitelnou úroveň ochrany proti vysoce proměnlivým a externě vyvolaným útokům. Dodavatel je schopen tato SLA standardně plnit a v praxi je plní, nicméně nelze vyloučit zcela výjimečné situace, kdy i přes vynaložení veškerého odborného a technického úsilí dojde ke krátkodobému nebo dílčímu nesplnění SLA, typicky v důsledku mimořádné intenzity nebo kombinace útokových vektorů.

Právě pro tyto výjimečné případy jsou v návrhu smlouvy sjednány smluvní pokuty, které představují předvídatelný, paušalizovaný a ekonomicky ocenitelný následek porušení SLA. Pokud je však vedle těchto smluvních pokut zachováno i právo objednatele domáhat se neomezené náhrady škody, dochází k situaci, kdy dodavatel nese riziko zcela nepředvídatelné a potenciálně neomezené škody i za marginální či krátkodobé odchylky od SLA, které jsou jinak smluvně ošetřeny sankčním mechanismem.

Dodavatel má za to, že v takovém nastavení přestává být rozlišováno mezi systémovým selháním a výjimečným excesem v rámci jinak řádně fungující služby. Neomezená náhrada škody se tak může uplatnit i v situaci, kdy je porušení povinností co do rozsahu i dopadu relativně omezené, avšak vzniklá tvrzená škoda na straně objednatele může být zcela nepředvídatelná a v extrémním nepoměru k hodnotě poskytovaného plnění. Takové riziko není dodavatel schopen rozumně ocenit ani pojistit a jeho přenesení na dodavatele může vést buď k výraznému navýšení nabídkové ceny, nebo k omezení hospodářské soutěže.

S ohledem na výše uvedené má dodavatel za to, že v případech porušení SLA, pro něž jsou sjednány smluvní pokuty, by měla smluvní pokuta plnit funkci primárního a předvídatelného nástroje kompenzace, a to zejména v situacích, kdy je SLA porušeno výjimečně a nikoliv systematicky. Zachování práva na neomezenou náhradu škody i v těchto případech se jeví jako nepřiměřené ve smyslu zásady přiměřenosti dle § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek (ZZVZ).

Dodavatel proto žádá změnu znění čl. 6 odst. 7 závazného návrhu smlouvy tak, že v rozsahu porušení povinností pokrytých SLA a sankcionovaných smluvními pokutami bude odpovědnost dodavatele za škodu přiměřeně omezena, případně že náhrada škody nebude uplatňována vedle smluvní pokuty za totožné porušení povinností.

Odpověď na dotaz č. 4

Zadavatel trvá na znění smlouvy.

Smluvní pokuta plní funkci paušalizované sankce, zatímco náhrada škody představuje samostatný zákonný institut. Zadavatel nepovažuje za přiměřené omezovat odpovědnost dodavatele za škodu vzniklou porušením jeho povinností, ani omezovat náhradu škody pouze na výši smluvních pokut, neboť předmětem plnění je kritická bezpečnostní služba (DDoS ochrana).

Zadavatel současně uvádí, že předmětem plnění je poskytování služby kybernetické bezpečnosti určené k ochraně kritických systémů regulovaného subjektu. Případné porušení smluvních povinností tak může mít dopady přesahující samotné technické nesplnění SLA parametrů, včetně provozních, regulatorních či reputačních následků.

Zadavatel nepřipouští úpravu ustanovení.

Dotaz č. 5

Čl. VII odst. 8 závazného návrhu smlouvy upravuje povinnosti poskytovatele při ukončení poskytování služby, zejména ve vztahu k „poskytování součinnosti ve vztahu k poskytovateli konektivity objednatele“. Z uvedeného ustanovení není zřejmé, co konkrétně má tato součinnost obnášet, jaké činnosti má poskytovatel vykonávat, v jakém rozsahu a na základě jakého vztahu k poskytovateli konektivity, který je samostatným smluvním partnerem objednatele.

Dodavatel má za to, že formulace je neurčitá a neumožňuje předem posoudit, jaké konkrétní povinnosti mu mají v souvislosti s přechodem služby vzniknout, zejména zda má jít pouze o obecnou koordinaci ukončení služby, nebo o aktivní zapojení do komunikace či technických kroků vůči třetí osobě, k níž dodavatel nemá žádný smluvní vztah. Takto nejasně vymezená povinnost vyvolává pochybnosti o rozsahu plnění a odpovědnosti dodavatele a může být problematická z hlediska transparentnosti zadávacích podmínek.

Dodavatel se proto dotazuje, zda zadavatel upřesní, co konkrétně rozumí součinností poskytovatele ve vztahu k poskytovateli konektivity objednatele podle čl. VII odst. 8 smlouvy.

Odpověď na dotaz č. 5

Zadavatel sděluje, že v případě požadavku na poskytnutí součinnosti se jedná o obecnou koordinaci ukončení služby, která zahrnuje zejména

- koordinaci technických změn při migraci nebo ukončení služby,
- součinnost při přesměrování provozu (routing/DNS/BGP dle architektury),
- poskytování technických informací nezbytných pro zachování kontinuity ochrany,
- účast na koordinačních jednáních mezi objednatelem a poskytovatelem konektivity.

Nejde o vznik smluvního vztahu mezi poskytovatelem a třetí stranou (poskytovatelem konektivity), ale o technickou součinnost vůči objednateli.

Zadavatel považuje obecné vymezení součinnosti při ukončení poskytované služby za dostatečné a v návrhu smlouvy jej neupravuje.

Dotaz č. 6

Dodavateli není zřejmé nastavení cenových podmínek v zadávací dokumentaci. Zadavatel požaduje uvedení měsíční ceny a současně celkové ceny za období 60 měsíců, přičemž zároveň stanoví, že smlouva automaticky zaniká okamžikem dosažení úhrad ve výši 3 000 000 Kč bez DPH. Takové nastavení vyvolává pochybnosti o smyslu uvedené klauzule, neboť její aplikace by fakticky předpokládala, že celková cena za 60 měsíců plnění může uvedený finanční limit přesáhnout. Pokud má však být celková cena za celé 60měsíční období limitem 3 000 000 Kč bez DPH nepřekročitelná, postrádá ustanovení o automatickém zániku smlouvy po vyčerpání této částky praktický význam. Dodavatel proto považuje zadávací podmínky v této části za vnitřně rozporné a požaduje jejich vysvětlení, zejména zda zadavatel předpokládá možnost sjednání celkové ceny za 60 měsíců vyšší než 3 000 000 Kč bez DPH, nebo zda má být tento limit považován za maximální celkovou cenu plnění.

Odpověď na dotaz č. 6

Zadavatel potvrzuje, že celková cena plnění za 60 měsíců je omezena částkou 3 000 000 Kč bez DPH, tento limit je maximální a nepřekročitelný.

Ustanovení o automatickém zániku smlouvy má význam jako kontrolní mechanismus čerpání - ochrana proti překročení finančního rámce při měsíční fakturaci.

Smlouva nepředpokládá možnost překročení tohoto limitu.

Dotaz č. 7

Zadavatel v návrhu smlouvy na více místech upravuje povinnosti dodavatele, které se svým obsahem přímo či nepřímo vztahují ke kybernetické bezpečnosti a poskytování regulované služby, a to zejména prostřednictvím požadavků na zajištění bezpečnosti poskytovaných služeb, prevence a řešení bezpečnostních incidentů, oznamovacích povinností a odpovědnosti za narušení bezpečnosti, přičemž v jednom případě je kybernetická bezpečnost výslovně zmíněna a v dalších ustanoveních je řešena nepřímo prostřednictvím definice bezpečnostního incidentu a souvisejících povinností dodavatele. Současně však ze zadávací dokumentace ani návrhu smlouvy nevyplývá, že by zadavatel výslovně stanovil, zda má být dodavatel považován za významného dodavatele ve smyslu právních předpisů upravujících kybernetickou bezpečnost, ani jaký konkrétní regulační režim na dodavatele v této souvislosti dopadá. Dodavatel má za to, že uvedená nejasnost může vyvolávat pochybnosti ohledně rozsahu povinností, které má dodavatel plnit, a tím i ohledně ocenění a řízení rizik spojených s plněním veřejné zakázky. Dodavatel se proto dotazuje, zda zadavatel potvrdí, že plnění předmětu veřejné zakázky nezakládá postavení dodavatele jako významného dodavatele regulované služby podle předpisů o kybernetické bezpečnosti, případně zda zadavatel zpřesní smluvní podmínky tak, aby bylo

jednoznačně zřejmé, z jakého regulatorního rámce zadavatel při formulaci bezpečnostních požadavků vychází.

Odpověď na dotaz č. 7

Zadavatel potvrzuje, že objednatel je regulovaným subjektem v oblasti kybernetické bezpečnosti (poskytovatelem regulované služby v režimu vyšších povinností jak je uvedeno v čl. II. odst. 3 návrhu smlouvy). Tato skutečnost sama o sobě automaticky z poskytovatele nečiní významného dodavatele ve smyslu právních předpisů o kybernetické bezpečnosti, nicméně plnění smlouvy musí splňovat bezpečnostní požadavky odpovídající režimu zadavatele. Pokud by měl být poskytovatel významným dodavatelem objednatel, bylo by to ve smlouvě výslovně uvedeno a současně by návrh smlouvy musel poskytovatele zavazovat k plnění celé řady dalších povinností podle předpisů o kybernetické bezpečnosti.

Zadavatel tak potvrzuje, že plnění předmětu nadepsané veřejné zakázky nezakládá postavení dodavatele jako významného dodavatele regulované služby podle předpisů o kybernetické bezpečnosti. Zadavatel však musí splňovat bezpečnostní požadavky stanovené pro poskytovatele regulované služby v režimu vyšších povinností podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, vyhlášky č. 408/2025 Sb., o regulovaných službách, a vyhlášky č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

Dotaz č. 8

Dodavatel se dotazuje na rozdíl mezi reakční dobou a zahájením mitigace uvedenými v příloze č. 1 zadávací dokumentace, části SLA. Z definic vyplývá, že reakční doba je stanovena jako čas od detekce incidentu do zahájení mitigace, přičemž zahájením mitigace je okamžik, kdy začne technické filtrování škodlivého provozu. Dodavatel proto není zřejmé, v čem má být praktický rozdíl mezi těmito dvěma dobami, když reakční doba končí právě zahájením mitigace. Dodavatel se proto dotazuje, zda zadavatel může tento rozdíl blíže vysvětlit, případně pojmy zpřesnit tak, aby bylo zřejmé, jaký samostatný význam mají.

Odpověď na dotaz č. 8

Zadavatel uvádí, že rozdíl mezi reakční dobou a zahájením mitigace je v tom, že reakční doba zahrnuje proces od detekce útoku k následnému rozhodnutí o technických opatřeních vedoucích k jeho eliminaci, zatímco okamžik zahájení mitigace je konkrétní technický okamžik spuštění ochranných opatření, ke kterým poskytovatel došel v rámci reakční doby. Jde tedy o vztah „proces vs. technická akce“, nikoli duplicitu.

Pokud v případě některého dodavatele reakční doba a čas zahájení mitigace splývá v jeden okamžik, jedná se o výhodu na straně takového dodavatele, není však třeba tyto dva pojmy slučovat v jeden.

Zadavatel má za to, že definice uvedených pojmů v návrhu smlouvy je jasná a srozumitelná a není nutné ji v návrhu smlouvy upřesňovat.

Dotaz č. 9

Z návrhu smlouvy vyplývá, že „chráněnou službou“ se rozumí veškeré informační, aplikační a síťové služby objednatel provozované na objednatel definovaných IP adresách, IP rozsazích nebo doménových jménech. Zadávací dokumentace však nikde konkrétně nevymezuje, které služby mají být skutečně chráněny, kde jsou provozovány, na jakých konektivitách se nacházejí ani jaký je jejich obvyklý objem legitimního („čistého“) provozu. Bez takové specifikace není možné objektivně navrhnout technické řešení, posoudit kapacitní nároky ani přiměřeně ocenit poskytovanou službu, protože rozsah a charakter chráněných služeb má přímý vliv na architekturu mitigace i na související provozní náklady. Doplní zadavatel zadávací dokumentaci o jednoznačnou specifikaci chráněných služeb, případně jejich rozsahu a základních provozních parametrů?

Odpověď na dotaz č. 9

Zadavatel nepovažuje za účelné uvádět detailní seznam chráněných služeb již v zadávací fázi z důvodu bezpečnostní citlivosti a možné změny infrastruktury.

Poskytovatel musí nacenit řešení na základě obecně známých modelů, přesná topologie konektivity není nutná pro stanovení nabídkové ceny, riziko variability konektivity je standardní součástí tržního rizika DDoS služeb a promítá se do SLA a ceny paušálně.

Zadavatel uvádí, že chráněné služby budou definovány prostřednictvím IP rozsahů, domén a systémů po uzavření smlouvy, přičemž konkrétní seznam objednatel poskytne bez zbytečného odkladu po uzavření smlouvy.

Dotaz č. 10

V technické specifikaci je stanoven test mitigace minimálně dvakrát ročně. Zadávací dokumentace však již neupravuje, zda se má jednat o test prováděný jednostranně dodavatelem, nebo o test realizovaný ve spolupráci se zadavatelem, ani zda je tento test zahrnut v nabídkové ceně, případně jaké součinnosti zadavatele se test týká. Dodavatel má za to, že bez jasného vymezení těchto bodů není zřejmý rozsah povinností dodavatele ani odpovědnost za případné dopady testu na provoz chráněných služeb. Upřesní zadavatel způsob provádění testů mitigace, rozsah součinnosti zadavatele a potvrdí, že testy nejsou součástí sjednané ceny a budou představovat samostatné plnění nad rámec smlouvy?

Odpověď na dotaz č. 10

Zadavatel uvádí, že testy budou prováděny ve spolupráci objednatele a poskytovatele, jedná se o plánované testy, nikoliv ad hoc zásahy do provozu, termíny budou předem dohodnuty. Součinnost objednatele zahrnuje zejména umožnění testovacího provozu. Obsah testu bude identický s reálným provozem v prostředí objednatele.

Zadavatel uvádí, že testy jsou součástí ceny plnění, nepředstavují samostatné plnění nad rámec smlouvy a nejde o samostatně hrazené služby.

Dotaz č. 11

SLA, konkrétně pojem „doba plné mitigace“, je definován jako čas od zahájení útoku do stabilizace chráněné služby. Ačkoli je v návrhu smlouvy tento pojem formálně vymezen, zadávací dokumentace již nestanoví, co se rozumí „stabilizací chráněné služby“ a podle jakých objektivních kritérií má být posuzováno její dosažení. Zejména není zřejmé, zda má jít o dosažení určité dostupnosti, doručení konkrétního objemu čistého provozu v Mbps, nebo jiný technický ukazatel. Dodavatel má za to, že přesné a měřitelné definice stabilizace nelze nikdy dosáhnout a že takto neurčitý požadavek může vést k nevyváženému přenosu rizik na dodavatele. Současně dodavatel upozorňuje, že z kombinace požadavků na „plnou mitigaci“ v řádu desítek minut, na vysokou dostupnost služby a na neomezenou odpovědnost za škodu v plné výši vyplývá faktický požadavek na garantování stoprocentní dostupnosti chráněných služeb i v průběhu DDoS útoků. Dodavatel má za to, že takový požadavek neodpovídá obvyklé tržní praxi v oblasti Anti-DDoS

Dodavatel proto navrhuje, aby bylo výslovně stanoveno, že stabilizací chráněné služby se rozumí stav, kdy jsou po zahájení mitigace aktivována předem dohodnutá technická opatření proti DDoS útoku, dochází k prokazatelnému oddělení škodlivého a legitimního provozu a legitimní provoz je doručován směrem k chráněné službě v obvyklém rozsahu odpovídajícím její běžné provozní charakteristice, a to bez další eskalace útoku na síťové úrovni. Splnění tohoto stavu je doložitelné prostřednictvím incidentního reportu poskytovatele, obsahujícího zejména čas detekce útoku, čas zahájení mitigace, popis použitých mitigačních opatření, průběh útoku, objem filtrování škodlivého provozu a potvrzení obnovení průchodu legitimního provozu.

Odpověď na dotaz č. 11

Zadavatel uvádí, že stabilizace chráněné služby zahrnuje zejména aktivaci odpovídajících mitigačních opatření, oddělení škodlivého a legitimního provozu a obnovení průchodu legitimního provozu směrem ke chráněné službě.

Stabilizací chráněné služby se rozumí stav, kdy výše uvedená opatření vedou k reálné použitelnosti chráněné služby, tj. kdy je legitimní provoz doručován způsobem umožňujícím její běžné využívání s přihlédnutím k povaze a intenzitě probíhajícího útoku. Cílem je eliminace dopadu útoku na chráněné služby a dosažení funkčního stavu chráněných služeb při zachování dostupnosti odpovídající sjednaným SLA parametrům, tedy dosažení stavu před útokem.

Splnění podmínek stabilizace chráněných služeb bude doloženo zejména incidentním reportem poskytovatele. Toto je poskytovatel schopen doložit standardní reportem poskytovaných služeb, např. propustnost datové sítě, ztrátovost packetu, rychlost konektivity apod.

Dotaz č. 12

Dodavatel se dotazuje na lhůtu pro podání nabídky uvedenou v zadávací dokumentaci, podle níž má být nabídka podána dne 8. 5. 2026. V této souvislosti dodavatel upozorňuje, že uvedený den je státním svátkem, a není proto zřejmé, zda se nejedná o administrativní pochybení. Vzhledem k nejasnosti zadání dodavatel žádá zadavatele o prodloužení lhůty pro podání nabídek nejméně o celou původní délku.

Odpověď na dotaz č. 12

Zadavatel uvádí, že lhůta podle výzvy k podání nabídky činila 10 dní od zveřejnění výzvy a její konec tak připadl na den 8. 5. 2026. Protože tento den je svátek, došlo by automaticky k posunu konce lhůty na nejbližší následující pracovní den, tedy na pondělí 11. 5. 2026.

Zadavatel současně již v rámci vysvětlení zadávací dokumentace č. 1 lhůtu pro podání nabídky prodloužil, a to do dne 13. 5. 2026 do 12:00 hodin.

Dotaz č. 13

K bodu II.3. návrhu Smlouvy máme následující dotaz: V souvislosti s poptávaným předmětem plnění uchazeč upozorňuje, že samotná dodávka, implementace a provoz poptávaného programového a HW vybavení negarantuje plnění povinností dle zákona o kybernetické bezpečnosti (ZKB). Zadavatel nadále bude muset v souladu se ZKB prostřednictvím vlastního útvaru bezpečnostní události vyhodnocovat a případně hlásit. Chápe uchazeč správně, že zadavatel si je této skutečnosti vědom a je si vědom i skutečnosti, že dodavatel nebude na základě veřejné zakázky za zadavatele plnit povinnosti dle ZKB?

Odpověď na dotaz č. 13

Zadavatel potvrzuje, že si je vědom svých povinností vyplývajících z právních předpisů upravujících kybernetickou bezpečnost, včetně povinností souvisejících s vyhodnocováním a případným hlášením bezpečnostních incidentů.

Zadavatel v návrhu smlouvy nepřevádí své povinnosti podle předpisů o kybernetické bezpečnosti na dodavatele. Dodavatel je však povinen poskytovat součinnost v rozsahu sjednaném smlouvou, zejména při řešení bezpečnostních incidentů souvisejících s poskytovanou službou.

Dotaz č. 14

K bodu II.4. návrhu Smlouvy máme následující dotaz: V souvislosti s poptávaným předmětem plnění uchazeč upozorňuje, že samotná dodávka, implementace a provoz poptávaného programového a HW vybavení je preventivním opatřením, které však negarantuje, že zařízení zadavatele nebudou předmětem kybernetického útoku, resp. že se takový útok podaří odvrátit. Uchazeč ani jakýkoliv jiný dodavatel s ohledem na rozmanitost a neustálý vývoj kybernetických útoků nemůže garantovat 100 % účinnost systému vůči všem kybernetickým útokům a nést jakoukoliv odpovědnost za případné újmy zadavatele vzniklé v souvislosti s kybernetickým útokem, když za ty zůstává i v souladu s právními předpisy plně odpovědný pachatel kybernetického útoku.

S ohledem na uvedené uchazeč žádá zadavatele o doplnění následujícího ustanovení do vzoru smlouvy: „Smluvní strany berou na vědomí a prohlašují, že dodavatel nenese odpovědnost za případnou újmu, kterou zadavatel utrpí v důsledku jakéhokoli kybernetického útoku směřovaného na

chráněná zařízení či vedeného prostřednictvím chráněných zařízení. Při poskytování konzultací dodavatel postupuje v souladu s doporučeními výrobce bezpečnosti platformy (SIEMu), aktuálními standardy na trhu (zejména doporučeními výrobců operačních systémů) a principy Best practice (Nejlepší praxe).“

Odpověď na dotaz č. 14

Zadavatel uvádí, že poskytování služby ochrany proti DDoS útokům nepředstavuje absolutní garanci zabránění všem kybernetickým útokům a jejich důsledkům. Odpovědnost poskytovatele se však vztahuje výlučně k plnění jeho smluvních povinností, zejména k poskytování služby s odbornou péčí a k dodržování sjednaných SLA parametrů. Zadavatel považuje za nepřijatelné obecné vyloučení odpovědnosti dodavatele za újmu vzniklou v souvislosti s porušením jeho smluvních povinností nebo nedodržením sjednaných SLA parametrů, tak jak vyplývá z jím navrženého textu. Odpovědnost za protiprávní jednání třetích osob, včetně pachatelů kybernetických útoků, tímto ustanovením není dotčena.

Zadavatel nepřipouští úpravu návrhu smlouvy.

Dotaz č. 15

K bodu II.7. návrhu Smlouvy máme následující dotaz, který je relevantní v případě, pokud má být součástí předmětu plnění veřejné zakázky i analytický nástroj SIEM sloužící k identifikaci kybernetických bezpečnostních událostí: Nástroj SIEM je SW produktem třetí strany, která nástroj provozuje a poskytuje k užití koncovým uživatelům dle vlastních smluvních a licenčních podmínek. V SIEMu jsou logy zpracovány na základě detekčních pravidel definovaných provozovatelem, a to v souladu s nastavením systému provedeným koncovým uživatelem (zadavatelem) v tenantu. Identifikované bezpečnostní události (alerty) jsou poté automaticky postoupeny prostřednictvím online ticketovacího nástroje ke zpracování SOC analytikům. Uchazeč v této souvislosti upozorňuje, že uchazeč ani žádný jiný dodavatel nemůže vlastnosti SW ani nastavení detekčních pravidel a zasílání alertů ovlivnit, protože vlastnosti či správná funkčnost SIEMu nemohou být ani předmětem jakékoliv garance či záruky ze strany dodavatele, resp. dodavatel může garantovat maximálně dodávku dle aktuálního portfolia provozovatele/výrobce SIEMu. Uchazeč dále upozorňuje zadavatele, že chyby (bugy) softwarového produktu SIEM odstraňuje pouze a výhradně provozovatel/výrobce SIEMu, přičemž licenční podmínky SIEMu a smluvní ujednání s provozovatelem/výrobce SIEMu neopravňují uchazeče k jakémukoliv zásahu do softwarového produktu SIEM, a naopak takový zásah uchazeče zcela vylučují.

V souvislosti s výše uvedeným se uchazeč táže, zda zadavatel může upravit ujednání čl. II. odst. 7 vzoru smlouvy, popř. doplní do předloženého vzoru smlouvy toto ujednání: „Veškeré licenční, servisní, reklamační, záruční a jiné podmínky ve vztahu k nástroji SIEM se řídí podmínkami provozovatele/výrobce SIEMu určenými pro daný produkt. Zadavatel se zavazuje užívat SIEM v souladu s podmínkami provozovatele/výrobce SIEMu. Smluvní strany činí nesporným, že vlastnosti či chyby (bugy) nástroje SIEM, jež je součástí plnění dle této smlouvy, jsou nastaveny, resp. odstraňovány v souladu s příslušnými podmínkami provozovatele/výrobce SIEMu a nepovažují se za vady plnění, pro které je zadavatel oprávněn uplatňovat práva z vadného plnění či náhradu škody po dodavateli.“?

Odpověď na dotaz č. 15

Zadavatel uvádí, že předmětem veřejné zakázky není dodávka analytického nástroje SIEM. Dotaz směřující k tomuto nástroji proto není pro tuto veřejnou zakázku relevantní.

Dotaz č. 16

K bodu VI.3. návrhu Smlouvy máme následující dotaz: Uchazeč žádá o vysvětlení, jaký je vztah smluvních pokut požadovaných zadavatelem dle čl. VI. odst. 2. a odst. 3., když z textu obou ustanovení se jeví, že jde o duplicitní smluvní pokutu za též porušení. Pokud se skutečně jedná o duplicitu, považuje uchazeč takové ujednání za zcela zjevně nepřiměřené a rozporné s požadavkem přiměřenosti dle § 6 odst. 1 ZZVZ, který je zadavatel povinen respektovat i v případě zadávání zakázky malého rozsahu. Uchazeč proto žádá o příslušnou úpravu textace ujednání, popř. jeho odstranění z textu smlouvy.

Odpověď na dotaz č. 16

Zadavatel uvádí, že ustanovení čl. VI odst. 2 a odst. 3 návrhu smlouvy sledují odlišné situace.

Čl. VI odst. 2 dopadá na případy prodlení se zahájením poskytování služby jako takové podle čl. II. odst. 1 návrhu smlouvy, a dále na případy, kdy služba nebude dodavatelem poskytována.

Čl. VI odst. 3 se vztahuje na porušení konkrétních SLA parametrů během poskytování služby.

Zadavatel současně uvádí, že za totožné porušení povinnosti nebude uplatňována duplicitní smluvní pokuta.

Dotaz č. 17

K bodu VI.7. návrhu Smlouvy máme následující dotaz: V souvislosti s ujednáním o smluvních pokutách dle čl. VI. vzoru smlouvy uchazeč uvádí, že závazek zaplatit smluvní pokutu dle požadavku zadavatele nevylučuje právo zadavatele na náhradu škody, a to v plné výši. Dle názoru uchazeče je takový požadavek nepřiměřený. Nelze po dodavateli spravedlivě požadovat, aby nesl odpovědnost za případnou škodu v plné výši. Důvodová zpráva k občanskému zákoníku na str. 569 uvádí, že rozsah náhrady škody podmiňuje její předvídatelnost. Dle názoru dodavatele nemůže být výše škody v daném případě předvídatelná, a může být zcela nepřiměřená míře rizika, kterou je dodavatel ochoten na sebe převzít při plnění veřejné zakázky. Požadavek na nijak nelimitovanou náhradu škody je nepřiměřený. Tím dochází k porušení zásady přiměřenosti uvedené v § 6 ZZVZ. Dodavatel nemůže dopředu výši škody předvídat a toto riziko musí promítat do nabídkové ceny. Uchazeč má za to, že ke stanovení neomezené odpovědnosti za škodu neopravňují zadavatele ani charakter, hodnota a význam zajišťovaných povinností, ani vzájemný poměr hodnoty zajišťovaného závazku a výše škody. Uchazeč apriori nepředpokládá, že bude porušovat své povinnosti ze smlouvy, ovšem přesto má za to, že je neomezená náhrada škody a výše zadavatelem požadovaných smluvních pokut nepřiměřená. Uchazeč si je vědom toho, že jednou ze základních povinností zadavatele je jednat s péčí řádného hospodáře, a tím i zajistit pokrytí eventuálních škod, jež by mu mohly vzniknout z porušení smluvního vztahu, nicméně z toho automaticky nevyplyvá povinnost požadovat nepřiměřeně vysoké smluvní pokuty a neomezenou náhradu škody po dodavateli ve veřejné zakázce. Uchazeč upozorňuje zadavatele, že také on i ostatní uchazeči o veřejnou zakázku jsou povinni jednat s péčí řádného hospodáře, přičemž jedinou možností jak sanovat nepřiměřené požadavky zadavatele je navýšit tzv. „risk budget“ tak, aby rizika vyplývající pro dodavatele ze souboru nepřiměřených požadavků dodavatele byla pokryta, resp. aby zisk z plnění veřejné zakázky odpovídal míře obchodního rizika. Náklady na tento risk budget budou rozprostřeny do nabídkové ceny. Zadavatel si musí být vědom toho, jaká maximální škoda by mohla teoreticky vzniknout, a jako řádný hospodář by mohl škodu a smluvní pokuty limitovat s přiměřenou rezervou. Za stávajících smluvních podmínek bude přitom zadavatel z veřejných prostředků sanovat náklady na risk budget v podobě vyšších nabídkových cen účastníků. Uchazeč s ohledem na uvedené žádá zadavatele o zvážení a přehodnocení požadavku na současné uplatnění smluvních sankcí i náhrady škody v plné výši.

Odpověď na dotaz č. 17

Zadavatel trvá na stávající úpravě odpovědnosti za škodu.

Zadavatel při nastavení smluvních podmínek zohlednil povahu chráněných služeb, regulatorní povinnosti zadavatele a význam zajištění jejich dostupnosti.

Smluvní pokuta a náhrada škody představují odlišné právní instituty s rozdílnou funkcí. Smluvní pokuta představuje paušalizovanou sankci za porušení smluvní povinnosti, zatímco náhrada škody slouží ke kompenzaci konkrétní újmy vzniklé v důsledku porušení povinností dodavatele. Samotná existence smluvní pokuty proto bez dalšího nevylučuje právo objednatele domáhat se náhrady skutečně vzniklé škody, zejména pokud by její rozsah přesahoval význam a účel sjednané smluvní pokuty.

Zadavatel opakovaně zdůrazňuje, že předmětem plnění jsou služby související se zajištěním kybernetické bezpečnosti a dostupnosti systémů povinného subjektu. Případné porušení smluvních povinností tak může mít dopady přesahující samotné nesplnění SLA parametrů, včetně provozních, regulatorních nebo reputačních následků, jejichž rozsah nelze předem paušálně předvídat ani objektivně vyčíslit.

Zadavatel současně nepředpokládá automatické uplatňování náhrady škody vedle smluvní pokuty v každém jednotlivém případě porušení smlouvy. Odpovědnost za škodu bude vždy posuzována individuálně, v souladu s příslušnými právními předpisy, zejména s ohledem na existenci porušení povinnosti, vznik škody, příčinnou souvislost a pravidla předvídatelnosti škody.

Zadavatel nepřipouští úpravu návrhu smlouvy.

Dotaz č. 18

K článku VII. návrhu Smlouvy máme následující dotaz: Uchazeč se při plnění veřejné zakázky stává zpracovatelem osobních údajů ve smyslu GDPR a z tohoto titulu je povinen chránit osobní údaje v souladu s GDPR a uzavřít se zadavatelem Smlouvu o zpracování osobních údajů.

Uchazeč se s ohledem na uvedené táže, zda zadavatel doplní zadávací dokumentaci o návrh Smlouvy o zpracování osobních údajů či zda umožní použití Smlouvy o zpracování osobních údajů, resp. doplnění smlouvy na plnění veřejné zakázky o Podmínky zpracování osobních údajů předložené dodavatelem?

Pro úplnost uchazeč upozorňuje, že povinnosti uzavření Smlouvy o zpracování osobních údajů je ve smyslu čl. 28 odst. 3 GDPR primárně odpovědností správce osobních údajů, tj. v tomto případě zadavatele.

Odpověď na dotaz č. 18

Zadavatel nepředpokládá, že by při běžném poskytování služby docházelo ke zpracování osobních údajů dodavatelem v postavení zpracovatele ve smyslu GDPR a není tedy nutné uzavírat zpracovatelskou smlouvu. Návrh smlouvy v čl. IV. zavazuje dodavatele k zachovávaní mlčenlivosti ohledně veškerých důvěrných informací, mezi které patří i informace chráněné GDPR. Zadavatel tuto úpravu považuje vzhledem k předmětu plnění veřejné zakázky za dostačující a přiměřenou.

Zadavatel doplňuje, že součástí zadávací dokumentace nebude smlouva o zpracování osobních údajů.

Dotaz č. 19

Závěrem uchazeč uvádí, že si je vědom, že zakázka je zadávána jako zakázka malého rozsahu na základě výjimky dle § 31 ZZVZ. I v takovém případě je však zadavatel povinen postupovat v souladu se zásadami přiměřenosti, transparentnosti, rovného zacházení a zákazu diskriminace dle § 6 odst. 1 a 2 ZZVZ. Shora naznačené nedostatky vzoru smlouvy přitom způsobují rozpor zadávacích podmínek se zásadou přiměřenosti. S ohledem na uvedené zadavatelem stanovené zadávací podmínky nepřipustně omezují veřejnou soutěž a zadavatel se tak vystavuje riziku obdržení menšího množství a méně výhodných nabídek, než pokud by si výše uvedené omezující podmínky nevymínil. Zároveň neexistuje legitimní a přiměřený důvod, aby zadavatel na výše uvedených sporných podmínkách trval. Pokud tedy zadavatel stanovením nepřiměřených zadávacích podmínek nedůvodně omezuje okruh potenciálních dodavatelů, postupuje při nakládání s veřejnými prostředky v rozporu s principy 3E a vystavuje se tak riziku postihu ze strany příslušného kontrolního orgánu.

Odpověď na dotaz č. 19

Zadavatel se s argumentací dodavatele seznámil, nicméně je přesvědčen, že zadávací podmínky odpovídají povaze a významu předmětu veřejné zakázky, regulatorním povinnostem zadavatele a požadavku na zajištění kontinuity a bezpečnosti chráněných služeb.

Zadavatel si je vědom skutečnosti, že veřejná zakázka je zadávána jako zakázka malého rozsahu, a při přípravě zadávacích podmínek respektoval zásady uvedené v § 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zejména zásadu přiměřenosti, transparentnosti a zákazu diskriminace.

Zadavatel současně uvádí, že požadavky obsažené v návrhu smlouvy reflektují charakter poskytovaných služeb, jejich význam pro provoz a dostupnost systémů zadavatele a rovněž regulatorní požadavky vyplývající z právních předpisů upravujících kybernetickou bezpečnost. Předmětem veřejné zakázky je poskytování bezpečnostní služby určené k ochraně kritických informačních a síťových služeb zadavatele před DDoS útoky, a tomu odpovídá i nastavení odpovědnostních mechanismů.

Zadavatel nepovažuje smluvní podmínky za nepřiměřené ani vybočující z obvyklého rámce pro obdobné bezpečnostní služby poskytované regulovaným subjektům. Zadavatel má současně za to, že zadávací podmínky umožňují podání hospodářsky soutěžitelných nabídek a bezdůvodně neomezují okruh potenciálních dodavatelů.

Zadavatel ve vysvětlení zadávací dokumentace reagoval na jednotlivé dotazy dodavatelů a upřesnil výklad vybraných ustanovení návrhu smlouvy, nepovažuje však za nutné ani účelné samotný návrh smlouvy měnit.

II. PRODLOUŽENÍ LHŮTY K PODÁNÍ NABÍDEK

S ohledem na vyšší počet dotazů k zadávací dokumentaci rozhodl zadavatel o dalším prodloužení lhůty k podání nabídek. Lhůta k podání nabídek prodloužená v rámci vysvětlení zadávací dokumentace č. 1 do 13. 5. 2026 do 12:00 hodin se tímto prodlužuje následovně:

Lhůta pro podání nabídek nově končí dne **18. 5. 2026 ve 12:00 hodin.**

S pozdravem

Ing. Jan Devetter

vedoucí odboru provozu IT

Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví

Ing. Jan

Devetter

Digitálně podepsal

Ing. Jan Devetter

Datum: 2026.05.07

15:47:35 +02'00'