Zadavatel:	**Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví**
Sídlo:	Roškotova 1225/1, 140 00 Praha 4
IČ:	47114321
Veřejná zakázka:	**„Smlouva pro realizaci penetračního testu“**
Ev. č. zadavatele:	**25_VERZAK_0026**

V Praze dne dle elektronického podpisu

ODPOVĚDI NA DOTAZY Č. 1 (VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE Č. 1 SPOJENÉ S JEJÍ ZMĚNOU/ÚPRAVOU) A PRODLOUŽENÍ LHŮTY K PODÁNÍ NABÍDEK Č. 1

I. ODPOVĚDI NA DOTAZY

Výše uvedený zadavatel obdržel ve dnech 6. 4. 2025, 8. 4. 2025, 9. 4. 2025, 11.4.2025, 13.4.2025 a 14.4.2025 následující dotazy k nadepsané veřejné zakázce, na který níže poskytuje své odpovědi.

Dotaz č. I.:
Zadavatel v čl. 3 zadávací dokumentace (dále též jen „ZD“) uvádí, že Dodavatelé (uchazeči) současně podáním nabídky berou na vědomí, že zadavatel je oprávněn před podpisem smlouvy s vítězným dodavatelem požadovat předložení kopie pojistné smlouvy dle čl. IV. odst. 5 návrhu smlouvy. Pojistná smlouva uchazeče je předmětem obchodního tajemství - postačí zadavateli pro prokázání pojištění odpovědnosti doložit potvrzení pojišťovny (certifikát o pojistném krytí), které obsahuje veškeré údaje o daném pojištění?

Odpověď na dotaz č. I.:
Zadavatel potvrzuje, že mu postačí k prokázání pojištění odpovědnosti doložit relevantní potvrzení pojišťovny (certifikát o pojistném krytí), pokud takovýto dokument obsahuje veškeré podstatné údaje o daném pojištění.

Dotaz č. II.:
Máme následující dotaz k čl. I. návrhu Smlouvy: S ohledem na povahu, způsob provedení a cíle penetračních testů a s ohledem k obecně závazným právním předpisům platných na území ČR uchazeč žádá o doplnění závazného vzoru smlouvy o následující ujednání: „Objednatel uděluje Poskytovateli souhlas k provedení penetračních testů, tj. simulace kybernetického útoku na systém Poskytovatele, dle této smlouvy. Provedení penetračních testů dle této smlouvy nebude považováno za kybernetickou bezpečnostní událost či kybernetický bezpečnostní incident ve smyslu § 7 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Provedení penetračních testů dle této smlouvy nebude považováno za porušení zabezpečení osobních údajů ve smyslu čl. 33 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR).“ V případě, že by zadavatel výše uvedené ujednání do vzoru smlouvy nedoplnil, mohla by být činnost dodavatele považována za nezákonnou a dodavatel by tak vystavoval riziku postihu ze strany orgánů veřejné moci.

Odpověď na dotaz č. II.:
Zadavatel se rozhodl akceptovat tento požadavek dodavatele (uchazeče) na doplnění textu návrhu smlouvy, a to v tomto mírně upraveném (zkráceném) znění. Viz nový čl. II. odst. 8 návrhu smlouvy:

„Provedení penetračních testů ve smyslu parametrů uvedených v této smlouvě nebude považováno za kybernetickou bezpečnostní událost či kybernetický bezpečnostní incident ve smyslu § 7 zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Provedení penetračních testů dle této smlouvy nebude považováno za porušení zabezpečení osobních údajů ve smyslu čl. 33 Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR).“

Dotaz č. III.:
Máme následující dotaz k odst. II. 6. návrhu Smlouvy, konkrétně k ustanovení „Stejně tak je Objednatel oprávněn objednat více služeb současně/souběžně." Může zadavatel upřesnit svoje plány na souběh testů? Uchazeč potřebuje znát maximální počet testů, které zadavatel reálně hodlá objednat souběžně – tato informace je klíčová pro plánování kapacit na straně uchazeče. Rovněž žádáme zadavatele o informaci, zda k takovému souběhu došlo v průběhu plnění smlouvy https://smlouvy.gov.cz/smlouva/26320659?backlink=crnzn, která je svými požadavky velmi podobná aktuálnímu zadávacímu řízení, a pokud ano, tak v jakém rozsahu (prosíme uvést konkrétní testy, které probíhaly souběžně s jinými včetně časování). Konečně uvádíme, že v praxi není souběžné provádění testů příliš obvyklé.

Odpověď na dotaz č. III.:
Zadavatel trvá na oprávněních, která mu umožňuje ustanovení čl. II. odst. 6 návrhu smlouvy, tzn. neobjednat některou či vůbec žádnou ze služeb či objednat více služeb současně. Současně zadavatel uvádí, že nepředpokládá objednání většího množství (např. všech) služeb současně. K předchozí smlouvě zadavatel upřesňuje, že během jejího plnění sice v jeden okamžik došlo k tomu, že plněny byly tři ze služeb současně, avšak jednalo se pouze o jejich krátký vzájemný překryv.

Dotaz č. IV.:
Máme následující dotaz k odst. VI. 2. návrhu Smlouvy: V souvislosti s ujednáním čl. VI. odst. 2. závazného vzoru smlouvy uchazeč žádá o vysvětlení, jaká autorská díla (alespoň typově), k nimž by zadavatel potřeboval udělit licenci, dle předpokladu zadavatele mohou být součástí plnění. Dle názoru uchazeče je uvedené smluvní ustanovení zavádějící a vzhledem k předmětu plnění irelevantní. Předmětem plnění ze strany dodavatele je provedení penetračních testů, tedy činnost jejímž výsledkem není jakýkoliv hmotný či nehmotný předmět autorského práva. S ohledem na uvedené uchazeč žádá o odstranění ujednání čl. VI. odst. 2. ze závazného vzoru smlouvy.

Odpověď na dotaz č. IV.:
Zadavatel uvádí, že uvedené je víceméně toliko „pojistkou" pro případy, kdy by případný dodavatel hypoteticky začal označovat např. své výstupy/zprávy z testování či cokoli, co by mělo vzniknout z plnění předmětné smlouvy, za autorské dílo. Uvedené ustanovení dodavatele (uchazeče) ve své podstatě nijak neomezuje, zadavatel nevidí důvod k jeho odstranění z návrhu smlouvy.

Dotaz č. V.:
Máme následující dotaz k odst. VII. 1. návrhu Smlouvy: V souvislosti s ujednáním čl. VII. závazného vzoru smlouvy uchazeč upozorňuje dodavatele, že v příloze č. 4 závazného vzoru smlouvy jsou osobní údaje řešeny toliko z pohledu ochrany důvěrnosti, resp. povinnosti mlčenlivosti. Součástí přílohy č. 4 není jakákoliv úprava ochrany osobních údajů ve smyslu GDPR. Dodavatel s ohledem na uvedené žádá zadavatele o sdělení, zda rámci poskytování plnění bude docházet ke zpracování osobních údajů, popř. k nahodilému přístupu k osobním údajům (tj. zejména zda cíle penetračních testů mohou osobní údaje obsahovat). V případě, kdy by v rámci poskytování plnění mělo dojít ke zpracování osobních údajů, dodavatel upozorňuje zadavatele, že v takovém případě může započít plnění až po uzavření smlouvy o zpracování osobních údajů. V souvislosti s tím se dodavatel táže, zda zadavatel disponuje vlastním vzorem smlouvy o zpracování osobních údajů, který by mohl doplnit do zadávací dokumentace. S odkazem na výše uvedené rovněž dodavatel žádá zadavatele o úpravu smluvních ujednání tak, aby v případě, kdy bude nezbytné uzavřít smlouvu o zpracování osobních údajů, mohla být smluvní pokuta dle čl. VIII. odst. 1 a postih dle čl. VIII. odst. 6 závazného vzoru smlouvy uplatněna až po uplynutí přiměřené lhůty k plnění počínaje uzavřením smlouvy o zpracování osobních údajů.

Odpověď na dotaz č. V.:
Zadavatel uvádí, že v rámci plnění nebude docházet ani k nahodilému zpracování osobních údajů. Z toho důvodu nepovažuje za nutné na smlouvě cokoli měnit. Mělo-li by hypoteticky přeci jen dojít k jakékoli změně v tomto ohledu, návrh smlouvy ve svém čl. VII. odst. 1 obsahuje závazek Poskytovatele uzavřít s Objednatelem případnou (odpovídající) smlouvu o zpracování osobních údajů.

Dotaz č. VI.:
Máme následující dotaz k odst. VIII. 10. návrhu Smlouvy: S ohledem na povahu a účel předmětu plnění veřejné zakázky a v souladu s dokumentem Penetrační testování – Úvod do problematiky ver. 1.2 ze dne 5. 3. 2024, zpracovaným Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB), dostupným zde: https://nukib.gov.cz/download/publikace/podpurne_materialy/2022-03- 07_Penetracni-testovani_v1.2.pdf uchazeč upozorňuje zadavatele na rizika penetračního testování, mezi která patří např.:

• při provádění automatizovaných testů může dojít k odmítnutí služby (denial of service) nebo k omezení provozu,
• pád systému,
• zahlcení sítě,
• spuštění tiskáren,
• při testování autentizace může dojít k zablokování účtů,
• získání přístupu do systému a k získání citlivých dat,
• získání přístupu jako reálný uživatel nebo administrátor,
• nestandardní chování aplikace,
• nechtěná aktivita (např. e-maily zákazníkům),
• průnik do cizích systémů (dodavatelé, soukromé, VPN, …)
• aktivace bezpečnostních mechanizmů aplikace/firewallu (může dojít k zaslání oznámení
• administrátorovi),
• zaplnění logovacího systému,
• poškození/zahlcení prvku nacházejícím se mezi útočícím a testovaným systémem,
• ztráta nebo znehodnocení dat,
• tvorba fiktivních registrací,
• shromažďování osobních údajů a jejich zpracovávání pro potřeby řádného provedení penetračního testování,
• při nedostatečné komunikaci může v organizaci nastat panika.

Uchazeč zároveň upozorňuje, že byť službu penetračního testování poskytuje v souladu se zásadami Best Practice a se zřetelem na minimalizaci rizik při zachování smyslu a účelu penetračního testování, nelze vzniku rizik a s tím souvisejícím případným škodám zcela předejít. S ohledem na uvedené a v souladu s doporučením NÚKIB dle výše citovaného dokumentu tak uchazeč žádá zadavatele o doplnění následujícího ustanovení do vzoru smlouvy: „Objednatel prohlašuje, že byl seznámen s typickými riziky provádění penetračních testů a bere na vědomí, že byť službu penetračního testování poskytuje Poskytovatel v souladu se zásadami Best Practice a se zřetelem na minimalizaci rizik při zachování smyslu a účelu penetračního testování, nelze vzniku rizik a s tím souvisejícím případným škodám zcela předejít. Smluvní strany výslovně vylučují odpovědnost Poskytovatele za jakoukoli újmu vzniklou v souvislosti s plněním povinností Poskytovatele dle smlouvy, nebyla-li způsobena úmyslně nebo z hrubé nedbalosti.“

<u>Odpověď na dotaz č. VI.:</u>
Zadavatel uvádí, že stávající návrh smlouvy kromě „obecného“ ustanovení čl. IV. odst. 3 („Poskytovatel se zavazuje k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod. Smluvní strany nesou odpovědnost za škodu dle platných právních předpisů a této smlouvy. Poskytovatel odpovídá za škodu rovněž v případě, že část služeb poskytne prostřednictvím poddodavatele.“) obsahuje též následující ustanovení, nacházející se v čl. IV. odst. 1 („Poskytovatel se zavazuje poskytovat plnění v souladu s platnými právními předpisy, jakož i v souladu se všemi relevantními normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy nebo jiná určující kritéria k zajištění, že užívané materiály, výrobky, postupy a služby vyhovují předmětu této smlouvy. Poskytovatel se současně zavazuje postupovat s odbornou péčí, podle svých nejlepších znalostí a schopností a podle pokynů Objednatele. V případě nevhodných pokynů Objednatele je Poskytovatel povinen Objednatele před provedením pokynů písemně upozornit na nevhodnost jeho pokynů, v opačném případě Poskytovatel nese odpovědnost za vady a škodu, které v důsledku nevhodných pokynů Objednatele vzniknou.“). Zadavatel z těchto důvodů nepovažuje požadavek dodavatele (uchazeče) za opodstatněný. Po úvaze naopak zadavatel doplnil do naposled citovaného ustanovení následující upřesňující větu: „V případě, že by plánovaná dílčí činnost v rámci

plnění smlouvy mohla způsobit jakoukoli škodu Objednateli, je Poskytovatel povinen na tuto skutečnost Objednatele předem prokazatelně upozornit tak, aby mohla být učiněna příslušná vhodná opatření či po dohodě zvolený případný alternativní, této smlouvě odpovídající způsob provedení daného dílčí činnosti“.

Dotaz č. VII.:
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 a zároveň se zásadou diskriminace, když zadavatel by v případě neupravení vzoru smlouvy zjevně upřednostňoval dodavatele, kteří porušují obecně závazné právní předpisy, resp. jsou ochotni zavázat se k plnění bez ohledu na zajištění souladu s platnými právními předpisy ČR. S ohledem na uvedené zadavatelem stanovené zadávací podmínky nepřípustně omezují veřejnou soutěž a zadavatel se tak vystavuje riziku obdržení menšího množství a méně výhodných nabídek. Pokud tedy zadavatel stanovením 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. VII.:
Zadavatel uvádí, že při přípravě veškeré dokumentace k předmětnému výběrovému řízení i k jiným výběrovým řízením přistupuje vždy odpovědně tak, aby naplnil všechny zásady uvedené v § odst. 1 až 3 ZZVZ. Zadavatel se tedy neztotožňuje s názorem dodavatele (uchazeče). Přesto v rámci dotazů č. II. a č. VI. návrh smlouvy doplnil, resp. zpřesnil. Pokud jde o ostatní dotazy, na všechny tyto zadavatel taktéž reaguje konkrétním způsobem a s odpovídajícím vysvětlením.

Dotaz č. VIII.:
Zadavatel stanovil jako jednu ze zadávacích podmínek požadavky na technickou kvalifikaci účastníků mimo jiné tak, že požaduje, aby součástí týmu účastníka byla mimo jiné Řídící osoba dodavatele pro celý projekt, která bude disponovat certifikací CompTIA Advanced Security Practicioner (CASP+). Zadavatel nicméně neuvádí žádné jiné další certifikace na stejné úrovni jako CASP+ a Účastníkovi tak není jednoznačně zřejmé, zda může potřebnou odbornou úroveň prokázat pracovníkem, který disponuje např. certifikací CISSP.
Účastník tedy žádá zadavatele o jednoznačné vysvětlení, zda jsou připuštěny i další jiné certifikace pro účely prokázání splnění technických kvalifikačních předpokladů Řídící osoby dodavatele pro celý projekt – a to certifikace stejné kvality jako uvedený CASP+, tj. zejména certifikace CISSP, resp. ostatní certifikace stejné kvality.
V případě, že zadavatel jinou takovou certifikaci nepřipouští, Účastník si dovoluje požádat zadavatele o změnu zadávacích podmínek tak, aby byla připuštěna i jiná certifikace stejné kvality – neboť omezení prokázání splnění technické kvalifikace pouze na jediný možný certifikát této profese – člena týmu pro plnění této veřejné zakázky je nadbytečně diskriminační. Účastníci jsou stejně kvalitně kvalifikovaní k plnění této veřejné zakázky, a to zejména na základě dlouholetých zkušeností plněním zakázek se stejným nebo obdobným předmětem plnění, přičemž kvalitu jeho služeb zajišťují profesní certifikace CEH, OSCP, CISSP. Včetně jejich kombinace. Případné zajištění informační bezpečnosti osvědčuje certifikát řízení informační bezpečnosti dle ČSN EN ISO/IEC 27001.
Předmětem plnění výše uvedené veřejné zakázky je poskytnutí služeb penetračního testování a bezpečnostní prověřování informačních systémů. Penetrační testy musí být provedeny podle definovaných standardů pro penetrační testování a certifikovanými specialisty. CompTIA Advanced Security Practitioner (CASP+) a ISC2 Certified Information Systems Security Professional (CISSP) jsou certifikace pokročilé úrovně, které ověřují dovednosti v udržování bezpečnosti informačních systémů a sítí. Certifikační zkouška CISSP využívá formát počítačového adaptivního testování (CAT) k vyhodnocení znalostí profesionála o strategii kybernetické bezpečnosti a praktických zkušeností s implementací. Hodnotí technické dovednosti pro návrh, provádění a řízení celkového stavu zabezpečení organizace. Je nejvhodnější pro zkušené bezpečnostní odborníky, manažery kybernetické bezpečnosti a vedoucí pracovníky. Certifikace CASP+ využívá otázky s výběrem odpovědí a otázky založené na výkonu k hodnocení schopnosti profesionála implementovat řešení, která zvýší odolnost organizace a zároveň bude dodržovat zásady a rámce kybernetické bezpečnosti. Nejvíce se hodí pro

pokročilé odborníky na kybernetickou bezpečnost, architekty a inženýry. Naplnění odborné úrovně Řídící osoby dodavatele pro celý projekt prostřednictvím certifikace stejné, srovnatelné, potažmo vyšší kvality, než je CompTIA Advanced Security Practicioner (CASP+) je zcela relevantní pro dosažení potřebné kvality realizačního týmu dodavatelů pro tuto veřejnou zakázku. Limitace pouze na certifikaci CompTIA Advanced Security Practicioner (CASP+) je požadavkem naopak nedůvodně omezujícím hospodářskou soutěž (diskriminačním).
S ohledem na výše uvedenou argumentaci žádá Účastník o úplné odstranění nadbytečně diskriminačního omezení účasti v tomto zadávacím řízení spočívajícím v požadavku na kvalifikaci takovém, aby účastník disponoval členem týmu s certifikací pouze CompTIA Advanced Security Practicioner (CASP+), a výslovně připustil certifikaci stejné či srovnatelné kvality, jako je CISSP a další.

Odpověď na dotaz č. VIII.:
Zadavatel v reakci na uvedený dotaz uvádí a tím i upravuje požadavek na certifikaci „Řídící osoby dodavatele pro celý projekt" tak, že alternativně [vedle „Certifikace CompTIA Advanced Security Practicioner (CASP+)"] uzná i předložení certifikátu CISSP.

Dotaz č. IX.:
Doba zahájení a odevzdání prací: je zapotřebí mít po podepsání do 30 dnů hotové penetrační testy cloud prostředí, nebo stačí pouze zahájit do 30 dnů penetrační testy cloud prostředí (Microsoft).

Odpověď na dotaz č. IX.:
Zadavatel uvádí, že dle čl. II. odst. 3 věty druhé a třetí návrhu smlouvy [„(…) *Objednatel písemně uplatní u Poskytovatele požadavek na provedení některé ze služeb uvedených v odstavci 1, resp. v příloze č. 1 této smlouvy (=vyzve jej k plnění) s tím, že Poskytovatel je povinen tuto službu provést ve lhůtě (počítáno ode dne doručení výzvy k plnění Poskytovateli) uvedené v příloze č. 1 této smlouvy u každé jednotlivé služby. V této lhůtě pro plnění je Poskytovatel povinen službu provést, a to kompletně (avšak zatím bez re-testu, předpokládá-li ho daná služba, viz následující odstavec), včetně výstupu testování (závěrečné zprávy).* (….)"], ve spojení s přílohou č. 1 návrhu smlouvy – Technická specifikace předmětu plnění, u služby č. 4 (Penetrační testování cloud prostředí) jednoznačně stanoví lhůtu pro provedení služby ode dne objednání 30 pracovních dnů (auditní procedury, vyhodnocení získaných informací a testování, závěrečná zpráva). Nejedná se v žádném případě o lhůtu k zahájení testování, ale k dokončení všech uvedených dílčích činností.

Dotaz č. X.:
Výstup testování: pokud má zadavatel jasnou představu o výstupu, kterou chce dodat, může poskytnout příklad nebo šablonu takového výstupu?

Odpověď na dotaz č. X.:
Zadavatel uvádí, že na str. 2 a 3 přílohy č. 1 návrhu smlouvy – Technická speficikace předmětu plnění, je popsána požadovaná struktura, resp. závazné náležitosti výstupu (závěrečné zprávy). Zadavatel z tohoto důvodu nepovažuje za nutné stanovovat konkrétní „šablonu" závěrečné zprávy.

Dotaz č. XI.:
Dobrý den, níže si dovoluji zaslat dotaz k veřejné zakázce. Jeden z potencionálních dodavatelů žádá Zadavatele o sdělení informace, zda trvá na doložení certifikace CASP+ , nebo zda bude dostačující (akceptováno) doložení certifikace typuCompTIA security+.

Odpověď na dotaz č. XI.:
Zadavatel uvádí, že trvá na doložení certifikace CASP+, eventuálně pak CISSP (viz odpověď na dotaz č. VIII.).

Dotaz č. XII.:

V zadávací dokumentaci je požadována certfikace "Microsoft 365 Certified: Enterprise Administrator Expert". Dovolujeme si Vás upozornit, že společnost Microsoft tuto certifikaci v září 2023 přejmenovala na "Microsoft 365 Certified: Administrator Expert" a původní název se již nepoužívá.

Z dostupných informací vyplývá, že obě certifikace jsou svým významem rovnocenné a ověřují odborné znalosti a dovednosti potřebné pro správu prostředí Microsoft 365 na expertní úrovni. Současná certifikace "Microsoft 365 Certified: Administrator Expert" navíc pokrývá komplexní spektrum administrace Microsoft 365 prostřednictvím zkoušky MS-102, která nahradila dřívější dvě zkoušky (MS-100 a MS-101) vyžadované pro certifikaci "Microsoft 365 Certified: Enterprise Administrator Expert". S ohledem na výše uvedené se tážeme, zda zadavatel uzná jako rovnocennou i certifikaci "Microsoft 365 Certified: Administrator Expert" pod jejím současným názvem.

Odpověď na dotaz č. XII.:
Zadavatel po posouzení věci uvádí, že bude akceptovat též certifikaci "Microsoft 365 Certified: Administrator Expert".

Dotaz č. XIII.:
Dobrý den, mám dotaz ohledně požadovaných certifikátů v rámci výběrového řízení 25_VERZAK_0026 "Smlouva pro realizaci penetračního testu". Společnost XXX, resp. její zaměstnanci mají následující certifikáty:
AWS Certfied Cloud Practitioner - 1 zaměstnanec
CEH - 5 zaměstnanců
eMAPT - 1 zaměstnanec
OSCP - 3 zaměstnanci
OSEP - 1 zaměstnanec
OSWA - 2 zaměstnanci
eJPT - 1 zaměstnanec

Jinými slovy, nemáme Vámi požadované certifikáty v plném rozsahu. Je to pro Vás KO kritérium v rámci podávání nabídek?

Odpověď na dotaz č. XIII.:
Zadavatel uvádí, že na svých požadavcích uvedených ve Výzvě k podání nabídky, se zohledněním výše poskytnutých odpovědí na dotazy č. VIII., č. XI. a č. XII., trvá.

II. PRODLOUŽENÍ LHŮTY K PODÁNÍ NABÍDEK

S ohledem na skutečnost, že zadavatel na základě dotazů dodavatelů přistoupil k úpravám v zadávací dokumentace, přičemž vzal i v potaz na své zdržení při odpovědi na tyto dotazy, rozhodl zadavatel o prodloužení lhůty k podání nabídek. Lhůta k podání nabídek původně stanovená do 16.4.2025 do 12:00 hodin se tímto prodlužuje následovně:

Lhůta pro podání nabídek nově končí dne **30.4.2025, ve 12:00 hodin**

S pozdravem

Ing. Jan Devetter

Digitálně podepsal Ing. Jan Devetter
Datum: 2025.04.14 15:59:05 +02'00'

Ing. Jan Devetter
vedoucí odboru provozu IT
Oborová zdravotní pojišťovna zaměstnanců bank, pojišťoven a stavebnictví