NÚKIB

ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK V OBLASTI ICT A KYBERNETICKÁ BEZPEČNOST

Metodický materiál

Verze 1.3, platná ke dni 30. 7. 2020

Obsah

Úvod

Účelem tohoto dokumentu je poskytnout veřejným zadavatelům, zejména správcům kritické informační infrastruktury (dále jen „KII“), významných informačních systémů (dále jen „VIS“) a informačních systémů základní služby (dále jen „ISZS“), podporu při zadávání veřejných zakázek v oblasti informačních a komunikačních technologií s cílem omezit negativní dopady, které může tento formalizovaný proces výběru dodavatele mít pro oblast kybernetické bezpečnosti. Cílem dokumentu není poskytnout komplexně zpracovaný postup pro zadávání veřejných zakázek, spíše je koncipován jako shrnutí možností, které zadavatelé pro řešení problematických částí mají.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 560

E-mail: regulace@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1 Vymezení problematiky

V době od nabytí účinnosti zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“), došlo Národním centrem kybernetické bezpečnosti k identifikaci některých bílých míst zajišťování kybernetické bezpečnosti. Jedním z těchto bílých míst bylo i nedostatečné a nesystematické řešení některých rozporů mezi zajišťováním kybernetické bezpečnosti a potřebou otevřené hospodářské soutěže při zadávání veřejných zakázek dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“).

Problémy byly identifikovány zejména v následujících oblastech:

- způsoby zohlednění požadavků vyplývajících z vyhlášky o kybernetické bezpečnosti v zadávacím řízení,
- omezování rizikových technologií,
- zamezení šíření bezpečnostní či jinak citlivé dokumentace v rámci zadávacího řízení,
- správné nastavení kvalifikačních předpokladů a jejich kontrola,
- kontrola a řízení poddodavatelů,
- plánování a náklady životního cyklu.

Dokument v následujících částech tyto problémy dále rozvádí a popisuje jejich možná řešení za současného respektování pravidel hospodářské soutěže.

2 Zohlednění požadavků vyplývajících z vyhlášky o kybernetické bezpečnosti v zadávacím řízení

Vyhláška 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, dále jen „VKB“), coby prováděcí právní předpis zákona o kybernetické bezpečnosti stanoví v podrobnostech požadavky na bezpečnostní opatření, která mají osoby spadající do působnosti zákona o kybernetické bezpečnosti zavádět. Ačkoli jde o povinnosti adresované primárně osobám uvedeným v § 3 zákona o kybernetické bezpečnosti, v návaznosti na § 4 odst. 4 a 7 zákona o kybernetické bezpečnosti jsou tyto osoby povinny požadavky vyplývající z bezpečnostních opatření zahrnout do smluv, které se svými dodavateli uzavírají. V případě výběru dodavatele prostřednictvím zadávacího řízení podle ZZVZ pak zadavatelům nezbyde než požadavky VKB promítnout i do zadávacích podmínek.

Zákon o kybernetické bezpečnosti stanovuje a VKB v podrobnostech upravuje širokou škálu opatření aplikovatelných jednak na předmět veřejné zakázky, jednak na osobu dodavatele. Obecně je přitom možné konstatovat, že ZZVZ umožňuje zadavatelům zanést do zadávacích podmínek jakékoli požadavky, jejichž potřeba je řádně odůvodněna (a které současně dostojí základním zásadám podle § 6 ZZVZ). Výjimkou je pouze limitace požadavků na kvalifikaci dodavatele. Všechna bezpečnostní opatření z VKB jsou podřaditelná pod některý z institutů upravených ZZVZ, ať již jde o kvalifikaci dodavatele, požadavky na předmět plnění nebo kritéria pro hodnocení nabídek. Záleží tedy pouze na potřebách zadavatele, jeho schopnosti řádně nadefinovat všechny podmínky pro přístup dodavatelů k zakázce a jeho kreativitě při využití možností, které mu ZZVZ nabízí. Nedávná rozhodovací praxe příslušného správního orgánu a správních soudů pak tyto závěry potvrzuje.[1]

Zákon o kybernetické bezpečnosti, VKB ani ZZVZ zadavatelům nestanoví, jakým konkrétním způsobem mají své bezpečnostní požadavky do zadávacích podmínek zahrnout. Lze předpokládat, že jedno bezpečnostní opatření bude v různých zadávacích řízeních koncipováno různě (např. některý zadavatel stanoví své požadavky jako nepřekročitelné technické podmínky, jiný zase bude tyto požadavky zohledňovat až v rámci hodnocení nabídek). V některých případech bude možné bezpečnostním požadavkům dokonce

[1] K tomu srov. zejm. rozhodovací praxi Úřadu pro ochranu hospodářské soutěže ve věcech zohlednění varování NÚKIB ze dne 17. 12. 2018 v zadávacím řízení, nebo níže citovaný rozsudek Nejvyššího správního soudu k požadavku na doložení certifikátu systému řízení bezpečnosti informací. Mimo oblast bezpečnosti informací lze odkázat i na relativně nedávnou rozhodovací praxi Úřadu pro ochranu hospodářské soutěže a Nejvyššího správního soudu týkající se problematiky vendor lock-in.

přizpůsobit samotný způsob zadání zakázky (např. za využití rozdělení veřejné zakázky na části a omezení počtu nabídek, které může jeden dodavatel podat).

Stejně tak citované předpisy nestanoví, jakou kvalitu a úroveň bezpečnostních opatření mají zadavatelé v rámci zadávacího řízení požadovat – tyto parametry budou výsledkem procesu hodnocení a řízení rizik a zohlednění konkrétních potřeb zadavatele. Je potřeba zdůraznit, že ZKB ani VKB nepředstavují univerzální povolení pro stanovení jakýchkoli bezpečnostních požadavků, volba konkrétní úrovně zabezpečení systémů a konkrétních bezpečnostních opatření bude založena především na řádně provedené analýze aktiv a s nimi souvisejících rizik a je výlučně v odpovědnosti povinné osoby (zadavatele), který si svůj postup musí řádně odůvodnit.

3 Omezení nákupu rizikových technologií

Informační a komunikační systémy by měly být zabezpečovány v co největší možné míře vzhledem ke specifickým hrozbám a rizikům, při současném rozumném vynaložení nákladů, které zabezpečení přináší. Správci KII, VIS a ISZS dle zákona o kybernetické bezpečnosti pak mají zákonnou povinnost[2] své systémy řádně zabezpečit. Součástí je pak i povinnost řídit rizika spojená se zajištěním bezpečnosti informací.

Tato povinnost klade na správce systémů nároky při zajištění dodávek, kdy musí minimalizovat rizika spojená s pořízením a využíváním cizích technologií. Při zadávání veřejných zakázek však lze vyloučit či omezit technologie pouze v souladu se ZZVZ tak, aby nedošlo k porušení práva hospodářské soutěže.

3.1 Jakým způsobem by měli zadavatelé postupovat, pokud chtějí pro plnění zakázky vyloučit či značně omezit využití rizikových technologií dodavatelem?

Omezit využití rizikových technologií dodavatelem lze v rámci zadávacího řízení několika způsoby.

3.1.1 Správné vymezení požadavků v rámci stanovení technických podmínek

Zadavatel může určit technologie (tj. technický popis způsobu provádění veřejné zakázky), které budou použity k plnění veřejné zakázky v rámci stanovení technických podmínek (§ 37 odst. 1, § 89 a násl. ZZVZ). Technické požadavky lze vymezit jak pozitivně (vyžadované technologie), tak negativně (zakázané technologie). Přitom ovšem podle § 36 odst. 1 ZZVZ platí, že zadávací podmínky nesmí být stanoveny tak, aby některým dodavatelům přímo nebo nepřímo zaručovaly konkurenční výhodu, nebo vytvářely bezdůvodné překážky hospodářské soutěže.

Zásadní je zde skutečnost, že se nesmí jednat o „bezdůvodné“ vytváření překážek hospodářské soutěže. Důvodová zpráva k ZZVZ zmiňuje, že některá omezení mohou být stanovena za účelem omezení rizik spojených s realizací zakázky, tedy může brát v potaz i bezpečnostní dopady použité technologie. Omezení hospodářské soutěže tedy možné je, ale jen tehdy, pokud jej lze obhájit objektivními skutečnostmi.

Za objektivní důvody pak lze považovat skutečnosti, kdy použití určité technologie je prokazatelně rizikovější, než použití jiné. To může vycházet např. z odborných testů, výzkumů aj. Tyto testy a výzkumy pak musí být dostatečně konkrétní a vztahující se k přímo posuzované technologii, nikoli obecně k výrobkům určitého výrobce atp.

[2] § 4 odst. 2 zákona o kybernetické bezpečnosti.

Důvodnost překážek hospodářské soutěži ve smyslu § 36 odst. 1 ZZVZ však bude vždy posuzována ve vztahu ke konkrétním specifikům zadavatele, rizikovost konkrétní technologie tedy bude jedním ze vstupů procesu hodnocení a řízení rizik (povinně prováděného osobami spadajícími do působnosti zákona o kybernetické bezpečnosti, dobrovolně prováděného dalšími subjekty).

Případná omezení je také potřeba formulovat věcně, nikoli osobně (vylučování konkrétních dodavatelů).

Lze dodat, že neúspěšní účastníci zadávacího řízení o zakázku mohou, a pravděpodobně také budou, podávat proti takovému postupu zadavatele námitky. Pokud je omezení vybraných technologií důvodné a podložené objektivními skutečnostmi, pak by tyto obavy neměly být překážkou využití daných oprávnění, zejména pak v případě správců a provozovatelů KII, VIS a ISZS, kterým je zákonem uložena povinnost řídit rizika a přijmout nutná opatření k jejich minimalizaci.

3.1.2 Bezpečnost jako kritérium kvality stanovené zadavatelem pro hodnocení nabídek

Není vyloučeno, aby bezpečnostní úroveň nabízeného plnění byla stanovena jako součást kritérií kvality stanovených zadavatelem pro hodnocení nabídek (§ 116 ZZVZ). V takovém případě nedochází a priori k vylučování určitých technologií, ale k hodnocení všech relevantních nabídek tak, aby objektivně bezpečnější technologie byly lépe hodnoceny. V tomto případě zadavatel musí v zadávací dokumentaci popsat, na základě jakých skutečností a jakým způsobem bude bezpečnost nabízeného plnění hodnocena.

ZZVZ uvádí názorně několik možných kritérií, která lze stanovit jako kritérium kvality, např. (i) technickou úroveň, (ii) organizaci, kvalifikaci nebo zkušenost osob, které se mají přímo podílet na plnění veřejné zakázky v případě, že na úroveň plnění má významný dopad kvalita těchto osob, (iii) úroveň servisních služeb včetně technické pomoci aj.

Kritéria kvality musí být vymezena tak, aby podle nich nabídky mohly být porovnatelné a naplnění kritérií ověřitelné. Je pak na zadavateli samotném, aby zhodnotil, jaká kritéria jsou ke konkrétní zakázce vhodná k porovnávání úrovně bezpečnosti jednotlivých nabídek.

3.2 Jak postupovat v případech, kdy je rizikovost dodávky svázaná s konkrétním dodavatelem?

V případech, kdy je riziko při výběru dodavatele spjato nikoli s technologií, ale s určitým dodavatelem, je nutné toto riziko také zohlednit v rámci zadávacího řízení. Možnosti jsou v tomto případě relativně omezené, zejména s ohledem na důraz, který ZZVZ klade na ochranu dodavatelů. I přesto nabízí ZZVZ k omezení rizikových dodavatelů několik institutů.

3.2.1 Využití kvalifikačních předpokladů

Obecně lze apelovat na plné využití možností, které dává ZZVZ co do požadavků na kvalifikaci dodavatele. Kvalifikaci lze sice požadovat pouze v oblastech, které ZZVZ stanovuje (§ 73 a násl. ZZVZ), nicméně jejich rozsah lze upravovat podle objektivních potřeb zadavatele. Správně nastavené kvalifikační předpoklady tak představují zákonem aprobovaný způsob omezení okruhu potenciálních dodavatelů.

Lze apelovat na zadavatele, aby kvalifikační kritéria stanovovali s vědomím, že jejich správné nastavení může oprávněně vyloučit z okruhu dodavatelů pro zadávací řízení ty dodavatele, kteří nejsou schopni zakázku realizovat.

Zatímco základní a profesní kvalifikace je dána relativně pevně, v rámci ekonomické a technické kvalifikace lze požadavky upravit dle potřeby zadavatele tak, ať jsou snížena rizika vyplývající z hlediska jeho ekonomických či technických možností, jak zakázku plnit (jedná se například o požadavek na seznam referenčních zakázek, přehled o řízení dodavatelského řetězce a systémy sledování dodavatelského řetězce aj.). Zadavatel je přitom povinen vyloučit ze zadávacího řízení vybraného dodavatele, jehož nabídka nesplňuje zadávací podmínky na základě § 48 odst. 8 ZZVZ.

Zvláštním oprávněním, které zadavatel v rámci posouzení kvalifikace má, je možnost považovat technickou kvalifikaci za neprokázanou, pokud zadavatel prokáže, že dodavatel má protichůdné zájmy, které by mohly negativně ovlivnit plnění veřejné zakázky. Opět je zde potřeba zdůraznit, že zadavatel musí takovou skutečnost prokázat, což může být v praxi značně obtížné. Nicméně z hlediska kybernetické bezpečnosti je potřebné tyto možnosti v případě existence vážných a podložených důvodů využívat.

3.2.2 Vyloučení účastníka zadávacího řízení pro nezpůsobilost

Účastníka zadávacího řízení lze také vyloučit na základě ustanovení § 48 odst. 5 ZZVZ. Zadavatel může vyloučit účastníka zadávacího řízení pro nezpůsobilost, pokud prokáže například, že (i) by výběrem či účastí dodavatele došlo ke střetu zájmů a tuto skutečnost nelze napravit jiným způsobem, než zrušením zadávacího řízení, nebo (ii) že se účastník dopustil v posledních třech letech od zahájení zadávacího řízení závažných nebo dlouhodobých pochybení při plnění dřívějšího závazku se zadavatelem (může jít i o zadavatele odlišného) která vedla k vzniku škody, předčasnému ukončení smluvního vztahu nebo jiným srovnatelným sankcím, aj.

Podstatným omezením oprávnění vyloučit účastníka zadávacího řízení v předmětném ustanovení je však opět nutnost veškeré důvody prokázat, což může v praxi činit problémy.

4 Zamezení šíření důvěrné dokumentace

Předpokladem řádného zadávacího procesu je umožnění účastníkům zadávacího řízení seznámit se se všemi informacemi, které jsou rozhodné pro vytvoření nabídky a stanovení její ceny. V případě dodávek ICT služeb pak mezi tyto informace mohou patřit i informace obsažené v interních předpisech či dokumentacích popisující konkrétní systémy a prvky jejich zabezpečení.

Poskytování těchto informací třetím subjektům však může být velmi výrazným bezpečnostním rizikem, jelikož mohou odhalit potenciálním útočníkům slabiny technického či organizačního zabezpečení systému včetně konkrétních technologií, které jsou využívány, a jejich nastavení. Z tohoto důvodu musí být zadavatelé schopni efektivně chránit tyto informace před dalším šířením.

4.1 Jaké možnosti ochrany důvěrných informací v rámci zadávacího řízení má zadavatel?

Základní institut, jenž slouží k ochraně důvěrné povahy informací, je obsažen v § 36 odst. 8 ZZVZ, dle kterého může zadavatel požadovat, aby dodavatel přijal přiměřená opatření k ochraně informací důvěrné povahy, které zadavatel poskytuje nebo zpřístupňuje v průběhu zadávacího řízení. Toto ustanovení je formulováno obecně, není tedy dán jednoznačný výčet takových opatření, jejich podoba je tudíž na uvážení zadavatele. Důvěrnou povahou informací se pak rozumí širší okruh informací, které zadavatel potřebuje chránit, nejedná se pouze o informace utajované.

Typicky lze na základě tohoto oprávnění požadovat po uchazeči přistoupení k závazku mlčenlivosti před předáním zadávací dokumentace. V závazku mlčenlivosti pak mohou být uvedeny podmínky využití poskytnutých informací, podmínky dalšího šíření těchto informací i sankční ustanovení za porušení daných povinností. Rozsah podmínek musí být přiměřený a musí odpovídat míře důvěrnosti informací.

Další možností je vyhradit si právo zpřístupnit informace pouze přímo u zadavatele. V takovém případě může být ta část zadávací dokumentace, která obsahuje důvěrné informace, zpřístupněna dodavatelům pouze fyzicky v místě, které zadavatel určil. Přitom lze vyžadovat identifikaci od osob, které si zadávací dokumentaci mají prohlížet. V úvahu také připadá zákaz kopírování či focení těch částí dokumentace, jejíž zveřejnění by mohlo zadavateli způsobit újmu, a dále další opatření, které mají za cíl zamezit šíření důvěrných informací.

Opět je zde nutné mít na paměti zásady zadávacího řízení, které rozsah opatření korigují. Veškerá opatření musí být přiměřená a nesmí bezdůvodně znesnadňovat dodavatelům získání informací, přičemž zadavatel musí pamatovat na adekvátní délku lhůt pro úkony dodavatelů. Zároveň musí veškeré stanovené podmínky dodavatelům umožňovat, aby se řádně seznámili se všem informacemi, které jsou z hlediska vytvoření relevantní nabídky podstatné.

V úvahu zde připadá také postup dle § 218 odst. 3 ZZVZ, podle kterého zadavatel nemusí uveřejnit informaci dle ZZVZ, pokud by její uveřejnění znamenalo mimo jiné rozpor s veřejným zájmem či jiným právním předpisem. Tento institut by mohl být využit v případě následně uveřejňovaných informací (písemná zpráva zadavatele, uzavřená smlouva).

V případě správců a provozovatelů KII, VIS a ISZS může být takovým důvodem i nutnost ochrany informací na základě povinností stanovených v zákoně o kybernetické bezpečnosti a konkretizovaných ve VKB, konkrétně pak povinností hodnotit a klasifikovat aktiva a následně je vhodným způsobem chránit (§ 4 VKB). V příloze č. 1 k VKB je pak přímo uvedeno, že zejména aktiva s úrovní hodnocení „Vysoká“ nebo „Kritická“ jsou tyto osoby povinny chránit před zveřejněním a vyžadují vysokou či nadstandardní míru ochrany.

Pokud by však měl být tento institut aplikován ve vztahu k zadávací dokumentaci (nebo jiným dokumentům uveřejňovaným v průběhu zadávacího řízení, které jsou způsobilé ovlivnit výsledek zadávacího řízení), měl by být spíše vykládán nikoli jako možnost informace neposkytnout, nýbrž jako povinnost nalézt jiné řešení, které zajistí co nejširší soutěž mezi dodavateli (např. za využití § 36 odst. 8 a § 96 odst. 2 ZZVZ).

V souvislosti s výše uvedeným je nutné také upozornit na § 96 odst. 2 ZZVZ, který v případě opatření dle § 36 odst. 8 ZZVZ dává možnost omezit zveřejnění příslušné části zadávací dokumentace na profilu zadavatele, a na § 211 odst. 3 písm. d) ZZVZ, který umožňuje z důvodu ochrany informací zvláště citlivé povahy také výjimku z jinak povinné elektronické komunikace mezi dodavateli a zadavatelem, pokud není možná rozumná úroveň zabezpečení v rámci běžně dostupných komunikačních nástrojů.

V případě, že by předmětem byly utajované informace, je pak samozřejmě možná aplikace § 104 písm. c) ZZVZ, popřípadě zadání veřejné zakázky v režimu výjimky podle § 29 písm. b) ZZVZ, příp. zadání veřejné zakázky v oblasti obrany či bezpečnosti ve smyslu § 187 ZZVZ.

4.2 Jaké druhy zadávacího řízení jsou z hlediska ochrany informací nejvhodnější a kdy je lze použít?

V případě veřejných zakázek na informační a komunikační technologie lze apelovat na využití vhodných druhů zadávacího řízení, které ZZVZ nabízí.

Lze tvrdit, že zadavatelé téměř nevyužívají jednacího řízení s uveřejněním či soutěžního dialogu i přesto, že právě tyto druhy mohou být nejvhodnější jak z hlediska výběru dodavatele, tak i z hlediska ochrany jejich zájmů.

4.2.1 Jednací řízení s uveřejněním

ZZVZ v § 60 uvádí, že jednací řízení s uveřejněním (dále jen „JŘSU“) lze v případě nadlimitních zakázek použít tehdy, pokud:

a) potřeby zadavatele nelze uspokojit bez úpravy na trhu dostupných plnění,
b) součástí plnění veřejné zakázky je návrh řešení nebo inovativní řešení,
c) veřejná zakázka nemůže být zadána bez předchozího jednání z důvodu zvláštních okolností vyplývajících z povahy, složitosti nebo právních a finančních podmínek spojených s předmětem veřejné zakázky, nebo
d) nelze stanovit technické podmínky odkazem na technické dokumenty podle § 90 odst. 1 a 2.

V řešeném ohledu je nejdůležitější zejména bod a) a b), tedy případy nákupu specifických dodávek či služeb ICT, které vyžadují určitou úpravu jinak na trhu dostupných plnění, popřípadě vyžadují návrh určitého řešení či inovativního řešení systému či služby vhodných pro specifickou potřebu zadavatele.

V případech podlimitních veřejných zakázek lze JŘSU dle § 52 písm. b) bod 1 ZZVZ využít vždy.

Prakticky může JŘSU pomoci zadavatelům postupně filtrovat vážné zájemce o zakázku a poskytovat jim potřebné informace postupně dle splnění předchozích částí zadávacího řízení. Více informací o využití JŘSU lze najít v ZZVZ, metodických materiálech Ministerstva pro místní rozvoj nebo literatuře k veřejným zakázkám.

4.2.2 Soutěžní dialog

Soutěžní dialog lze použít za stejných podmínek, jako lze použít JŘSU, nicméně účel je odlišný. Zatímco u JŘSU má zadavatel představu o finálním výsledku zakázky, u soutěžního dialogu vhodné řešení nezná a společně s účastníky se tak snaží nalézt řešení způsobilé splnit jeho potřeby.

Svým vymezením je tak vhodný k zadávání zakázek na dodávku specifických systémů připravených na míru konkrétní organizaci. Bezpečnostní aspekty pak mohou být předmětem jednání, přičemž i zde mohou být citlivé informace, které jsou potřebné pro stanovení nabídky, poskytovány postupně v závislosti na fázi řízení.

Oproti případům JŘSU není pro soutěžní dialog stanovena možnost ve smyslu § 52 písm. b) bod 1 ZZVZ.

Více informací o využití soutěžního dialogu lze najít v ZZVZ, metodických materiálech Ministerstva pro místní rozvoj nebo literatuře k veřejným zakázkám.

5 Kritéria kvalifikace a jejich kontrola

Jelikož jsou VIS, KII a ISZS systémy, které přímo ovlivňují bezpečnost České republiky, je vysoce žádoucí, aby dodavatelé splňovali potřebná kritéria kvalifikace pro účast v zadávacím řízení. Těmito předpoklady jsou mj. i požadavky na řízení bezpečnosti informací. Vedle formálního doložení je poté nutná i kontrola jejich reálného plnění. Kritéria kvalifikace je nutné správně nastavit i v případě dalších informačních a komunikačních systémů.

5.1 Lze požadovat po dodavatelích i doložení uznávaných certifikátů dokládajících splnění bezpečnostních požadavků (např. certifikát ISO řady 27000 apod.)?

Ačkoli dosavadní rozhodovací praxe Úřadu pro ochranu hospodářské soutěže požadování jiných než zákonem výslovně uvedených certifikátů zapovídala, Nejvyšší správní soud svým rozsudkem ze dne 25. 9. 2019, č. j. 6 As 113/2019-32[3] jasně deklaroval, že požadavek na doložení systému managementu bezpečnosti informací v organizaci je akceptovatelný, pokud má požadavek na dodržování příslušné technické normy úzkou souvislost s kvalitou poskytovaného plnění. Nejvyšší správní soud, při zohlednění specifik posuzovaného případu, pak nepovažuje za nezákonný požadavek zadavatele na doložení příslušné ochrany informací ze strany dodavatele, pokud se tento dodavatel může z povahy věci dostat k citlivým informacím, na jejichž ochraně existuje veřejný zájem.

Současně je možné, pokud je to odůvodněno předmětem veřejné zakázky, požadovat po dodavatelích plnění jednotlivých požadavků obsažených v normách týkajících se zajištění systému řízení bezpečnosti informací. U veřejné zakázky zadávané v nadlimitním režimu je nutné se držet zákonem stanovených mantinelů pro kvalifikační kritéria (zadavatel nemůže nastavit jiná kritéria kvalifikace, než stanovuje ZZVZ), u podlimitní veřejné zakázky zadávané ve zjednodušeném podlimitním řízení je naopak možné po účastnících zadávacího řízení požadovat i kritéria kvalifikace nad rámec stanovený v § 73 až § 80 ZZVZ. Takto nastavená kritéria musí být odůvodněná.

Požadavky založené na normách týkajících se zajištění systému řízení bezpečnosti informací se budou v mnoha případech krýt s požadavky na naplnění kritérií určených v zákoně o kybernetické bezpečnosti a VKB. Plnění povinností stanovených povinným osobám zákonem, potažmo jeho prováděcím právním předpisem, pak z povahy věci (i při zohlednění § 4 odst. 4 a 7 zákona o kybernetické bezpečnosti) nemůže být považováno za neodůvodněné omezování hospodářské soutěže.

[3] Text rozsudku je dostupný zde: http://www.nssoud.cz/files/SOUDNI_VYKON/2019/0113_6As__1900032_20190926140638_20191010100024_prevedeno.pdf.

5.2 Lze v rámci zadávacího řízení provést „zákaznický audit“, tedy reálnou kontrolu plnění veškerých požadavků kladených na dodavatele? Lze na základě výsledků tohoto auditu vyloučit účastníka zadávacího řízení i přesto, že formální podklady netrpí žádnou vadou?

Při posouzení splnění podmínek účasti nebo hodnocení nabídek zadavatel vychází primárně z údajů poskytnutých dodavatelem, ale může si jejich věrohodnost ověřit nebo si je opatřit sám, což je výslovně stanoveno § 39 odst. 5 ZZVZ. Zadavatel zároveň může (i opakovaně) žádat objasnění a doplnění dalších či chybějících údajů, dokladů, vzorků nebo modelů dle § 46 odst. 1 ZZVZ. K ověření nabídek je tedy možné použít jakékoli vhodné prostředky, včetně zákaznického auditu. Omezení lze spatřovat pouze v základních zásadách zadávání veřejných zakázek dle § 6 ZZVZ.

Audit může být proveden kdykoliv v průběhu zadávacího řízení. Není také vyloučeno, aby zadavatel postupoval dle § 104 odst. 1 ZZVZ, a vyžádal si před uzavřením smlouvy předložení dokladů (mohlo by jít např. o doklady o zkoušce či prověrce vztahující se k plnění veřejné zakázky) nebo předložení vzorků či úspěšný výsledek zkoušky těchto vzorků. Je přitom možné, aby zkoušky prováděl zadavatel či třetí subjekt. Zjištění třetího subjektu – auditora jsou ve vztahu k účastníku zadávacího řízení zjištěními zadavatele.

Zadavatel je oprávněn vyloučit účastníka zadávacího řízení, jehož nabídka je sice formálně v pořádku, ale jím uváděné údaje neodpovídají skutečnosti, a to na základě § 48 odst. 2 písm. c) ZZVZ (záleží však i na formulaci požadavků v zadávacích podmínkách, zejm. jestli zadavatel požaduje pouhé vlastnictví příslušného osvědčení, či zda požaduje splnění určitých požadavků, jež je možné doložit mj. předložením příslušného osvědčením).

5.3 Jakým způsobem může zadavatel zjistit o případném dodavateli informace podle § 48 odst. 5 písm. d) nebo f), tedy zda se účastník zadávacího řízení nedopustil v posledních 3 letech před zahájením zadávacího řízení závažných nebo dlouhodobých pochybení při plnění dřívějšího smluvního vztahu s jiným veřejným zadavatelem nebo závažného profesního pochybení, které zpochybňuje jeho důvěryhodnost?

Zákon zadavatele nijak neomezuje ve způsobu zjišťování informací použitelných k posouzení skutečnosti dle § 48 odst. 5 písm. d) a f) ZZVZ. Záleží tedy na zadavateli, jaké zdroje pro zjišťování informací nalezne. Lze např. uvažovat o kontaktování známých příjemců služeb či dodávek účastníka zadávacího řízení. Má-li zadavatel na základě takových informací zasáhnout do účasti dodavatele v zadávacím řízení, musí zajistit, aby tyto informace byly průkazné.

6 Řízení poddodavatelů v rámci veřejných zakázek

Vzhledem k povaze informačních a komunikačních systémů může být poskytování dodávek ICT prostřednictvím poddodavatelů rizikem, které musí správce (potažmo provozovatel) informačního nebo komunikačního systému řídit, popřípadě by jej v některých případech neměl připustit. ZZVZ však nepřipouští absolutní zákaz plnění zakázky prostřednictvím poddodavatelů.

6.1 Lze v některých specifických případech vyloučit, popřípadě omezit plnění zakázky prostřednictvím poddodavatele?

Omezení plnění zakázky poddodavateli je možné pouze dle § 105 odst. 2 ZZVZ, a to v případě veřejné zakázky na služby nebo stavební práce nebo v případě veřejné zakázky na dodávky zahrnující umístění nebo montáž. Zadavatel v takovém případě v zadávací dokumentaci určí významné činnosti při plnění veřejné zakázky, u nichž požaduje, aby byly plněny pouze vybraným dodavatelem. Je přitom vhodné zdůraznit, že rozsah významné části zakázky není stanoven a ZZVZ tak dává zadavateli možnost takto určit značnou část zakázky; v takovém případě je velmi důležité mít toto určení rozumně odůvodněno pro případný přezkum. Využití tohoto oprávnění z bezpečnostních důvodů je bezpochyby možné.

6.2 Jakým způsobem lze řídit a kontrolovat poddodavatele již v průběhu zadávacího řízení?

Vedle určení významné části zakázky, která bude plněna pouze konkrétním dodavatelem, je možné požadovat po účastnících zadávacího řízení seznam všech poddodavatelů, kteří se budou plnění zakázky účastnit, a části, které mají plnit; vyjma určené části, kterou musí dodavatel plnit sám, může být tento seznam dodavatelem měněn. K získání úplného přehledu o poddodavatelích zapojených do plnění veřejné zakázky může dojít až v průběhu plnění zakázky skrze institut upravený v § 105 odst. 3., resp. odst. 4 ZZVZ. Využití této možnosti by mělo být uvedeno v zadávací dokumentaci.

Samozřejmý je i požadavek na splnění základní a profesní způsobilosti poddodavatelů v tom rozsahu, jaký je pro plnění jejich částí zakázky podstatný. Stejně jako u účastníka zadávacího řízení je pak možné učinit kontrolu, zdali tvrzené skutečnosti o kvalifikaci odpovídají realitě.

Zásadní je také úprava vztahů zadavatele, dodavatele a poddodavatelů ve smlouvě, která by měla přesně stanovit, jak budou probíhat práce s poddodavateli, jak bude probíhat komunikace s nimi, zadávání práce a kontrola. Smlouva by také měla obsahovat efektivní sankční ustanovení pro případ porušení povinností.

7 Plánování a náklady životního cyklu

Změna dodavatele ICT může být pro správce (potažmo provozovatele) nákladným a náročným procesem, zejména v případech, kdy zasahují komplexní a komplikované systémy, které jsou uzpůsobeny na míru specifické činnosti organizace. Zadavatelé často narážejí na problémy plynoucí z potřeby opětovného soutěžení dodavatelů; jedná se o náklady spojené se sníženou efektivitou pracovníků, kteří jsou nuceni věnovat více času komunikaci s pracovníky nového dodavatele nebo s učením se v novém prostředí. Jedná se také o bezpečnostní aspekt, kdy „ladění" nového systému může přinášet bezpečnostní rizika. V neposlední řadě pak případná výměna dodavatelů musí brát v potaz i riziko, které souvisí s šířením vědomostí a know-how o konkrétním systému na další subjekt a jeho zaměstnance.

7.1 Lze zohlednit nákladové a bezpečnostní hledisko při posuzování nabídek jednotlivých dodavatelů?

Zohlednění nákladových či bezpečnostních hledisek je možné v rámci hodnocení nabídek, která by musela být zakomponována v kritériích kvality ve smyslu § 116 ZZVZ nebo započtena do nákladů životního cyklu, dle § 117 ZZVZ. Dosavadní dodavatel však nemůže být bez dalšího zvýhodňován.

7.2 Lze poptat upgrade systému, aniž by takový postup představoval neodůvodněné zvýhodnění stávajícího dodavatele?

Pokud zadavatel shledá, že jím používaný systém již nevyhovuje všem požadavkům, resp. že je potřeba jej upravit, modernizovat či rozšířit, není nezbytné za každou cenu upřednostňovat co nejširší hospodářskou soutěž a poptávat celý systém znovu. Pokud je požadavek zadavatele na zachování dosavadního systému (resp. zákaz migrace dat do nového systému, který s tím současným nekoresponduje) stanoven jednoznačně, má své logické opodstatnění a lze jej zdůvodnit s ohledem na předmět veřejné zakázky a s přihlédnutím k charakteru a účelu poptávaného plnění (při současném zohlednění základních zásad zadávání), lze takový požadavek vznesený v otevřeném řízení považovat za oprávněný.[4]

Uvedené je však třeba důsledně odlišovat od situací, kdy zadavatelé vědomě zapříčiní uzamčení se ve smluvním vztahu s konkrétním dodavatelem a následně se na tento vendor lock-in odvolávají při zadávání navazujících veřejných zakázek bez řádné soutěže.[5]

[4] K tomu srov. rozsudek Nejvyššího správního soudu ze dne 15. února 2018, č. j. 5 As 26/2017 – 22, dostupný zde: http://www.nssoud.cz/files/SOUDNI_VYKON/2017/0026_5As__1700022_20180221104537_20180221220016_prevedeno.pdf.

[5] K tomu srov. především bohatou rozhodovací praxi Úřadu pro ochranu hospodářské soutěže k institutu jednacího řízení bez uveřejnění.

7.3 Jaké možnosti má zadavatel pro případnou eliminaci výše uvedených problémů?

V této souvislosti je důležité apelovat na pečlivé plánování zadávání veřejných zakázek. Zadavatel musí počítat s tím, že v případě ukončení smlouvy může dojít k výměně dodavatele a s tím spojeným provozním komplikacím. Je tedy vhodné smlouvy uzavírat na přiměřenou dobu, zahrnout do předmětu veřejné zakázky kromě dodání nového informačního systému i jeho další rozvoj a technickou podporu. V úvahu přichází i vyhrazení možnosti případného prodloužení smlouvy v souladu s § 100 ZZVZ.

V zadávacích podmínkách pak lze stanovit např. požadavek, že dodavatel buď poskytne zdrojové kódy, nebo dodá software běžně dostupný na trhu, nebo dodá otevřený (open source) software[6], nebo požadavek, že proprietární software musí být nabízen na území České republiky několika na sobě nezávislými a vzájemně nepropojenými subjekty, které zároveň musí být oprávněny takový software upravovat[7], nebo požadavek na kompatibilitu poptávaných přístrojů se spotřebním materiálem od více různých výrobců obchodovaných na českém trhu po dobu trvání záruky a pozáručního servisu[8].

Zadavatel by současně měl zabránit situaci, kdy bude dosavadní dodavatel ztěžovat ukončení smluvního vztahu. Pro tento účel je podstatné si v rámci smluvních podmínek tyto otázky pečlivě upravit (zejména pak vlastnictví zdrojových kódů, předání dat v čitelné podobě, úpravu práv duševního vlastnictví aj.). Tzv. „exit strategy“ by měly vždy být součástí plánování veřejné zakázky.

[6] Viz rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 27. 2. 2018, č. j. ÚOHS-S0002/2018/VZ-06048/2018/511/ŠNo, které bylo potvrzeno rozhodnutím předsedy úřadu.
[7] Viz rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 11. 11. 2019, č. j. ÚOHS-S0361/2019/VZ-30614/2019/532/Loh, které bylo potvrzeno rozhodnutím předsedy úřadu.
[8] Viz rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 5. 4 2018, č. j. ÚOHS-S0061/2018/VZ-10030/2018/531/ESt, které bylo potvrzeno rozhodnutím předsedy úřadu.

8 Obecná doporučení

Plně využívejte možnosti, které Vám ZZVZ dává

ZZVZ nabízí zadavatelům různé možnosti, jak chránit své zájmy. Tyto jsou však často zadavateli nevyužity. Jedná se například o možnost ochrany citlivých informací, které jsou součástí zadávací dokumentace nebo možnost postupné filtrace vážných a schopných dodavatelů v rámci soutěžního dialogu nebo jednacího řízení s uveřejněním aj. Lze apelovat, aby byli zadavatelé plně seznámení se všemi možnostmi, které jim ZZVZ při provádění veřejných zakázek nabízí.

Odůvodněte si každý krok zadávacího řízení

Zadávací řízení je velmi formální proces, který klade značné nároky na zadavatele co do naplnění zákonných požadavků. Obecně však platí, že není cílem ZZVZ zadavatele pouze svazovat pravidly ve prospěch rovné hospodářské soutěže, nýbrž zadavatelům dává i možnosti, jak chránit své zájmy. Tyto však musí být podloženy logickými a pevnými argumenty.

Proto lze apelovat, aby byl každý krok zadavatele odůvodněný, odůvodnitelný a řádně zdokumentovaný. Pokud zadavatel bude schopen rozumně a věcně zdůvodnit každý svůj krok v rámci zadávacího řízení, přináší mu to značnou výhodu při případném přezkumu a dokáže urychlit celý přezkumný proces.

Plňte řádně povinnosti vyplývající ze zákona o kybernetické bezpečnosti

ZZVZ říká „jak“ mají zadavatelé své nákupy provést, nikoli „co“ mají zadavatelé poptávat. Naopak zákon o kybernetické bezpečnosti a jeho prováděcí vyhláška regulují kvalitativní stránku informačních systémů a zařízení, které zadavatelé používají a poptávají. Požadavky na předmět plnění veřejné zakázky založené na řádném plnění povinností vyplývajících ze zákona o kybernetické bezpečnosti, zejm. na řádně provedeném procesu řízení rizik a výběru bezpečnostních opatření k zajištění požadované úrovně kybernetické bezpečnosti, pak nemohou být z podstaty věci (stejně jako v případě všech dalších požadavků zadavatelů založených na plnění jejich zákonných povinností) považovány za neodůvodněné.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
12. 2. 2018	1.0	odd. NSP, odd. RAP	Vytvoření dokumentu
12. 11. 2018	1.1	Odb. regulace	Grafické úpravy dokumentu a aktualizace podkapitoly 3.1 (původní podkapitola 4.1)
28. 1. 2019	1.2	Odb. regulace	Změna kontaktních údajů
30. 7. 2020	1.3	Odb. regulace	Vložení současné kapitoly 2, aktualizace podkapitoly 5.1 (původní podkapitola 4.1), vložení podkapitoly 7.2, aktualizace podkapitoly 7.3 (původní podkapitola 7.2) a kapitoly 8, dílčí úpravy neměnící celkový charakter textu