

28. 1. 2020

Vezměte, prosíme, na vědomí, že text článku odpovídá platné právní úpravě ke dni publikace.

Veřejné zakázky a kybernetická bezpečnost

Řada subjektů, které mají povinnosti podle zákona č. [181/2014](#) Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZKB“), jsou současně veřejní zadavatelé podle zákona č. [134/2016](#) Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“). Některá bezpečnostní opatření, která jsou tyto subjekty dle ZKB v rozsahu nezbytném pro zajištění kybernetické bezpečnosti povinny zavést a provádět, mohou sama o sobě znamenat rozpor se ZZVZ.

Zejména se může jednat o rozpor se zásadou zákazu diskriminace a ustanovením § 36 odst. 1 ZZVZ, podle které zadávací podmínky nesmí být stanoveny tak, aby určitým dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže.

Veřejní zadavatelé, kteří jsou současně povinnými osobami dle ZKB (nebude-li dále výslovně řečeno jinak, rozumí se pod pojmem „veřejný zadavatel“ právě takový veřejný zadavatel), jsou dle § 4 odst. 4 ZKB povinni při výběru dodavatele zohlednit požadavky vyplývající z bezpečnostních opatření podle ZKB. Nejedná se tedy o možnost pro tyto veřejné zadavatele, ale o povinnost. Veřejní zadavatelé se tím mohou ocitnout mezi dvěma mlýnskými kameny.

Zohlednění požadavků bezpečnostních opatření v zadávacích podmínkách, je-li v míře nezbytné, nelze dle § 4 odst. 4 ZKB považovat za nezákonné omezení hospodářské soutěže ani za neodůvodněnou překážku hospodářské soutěže. Bez ohledu na toto ustanovení ZKB již samotný ZZVZ ve svém § 36 připouští, aby zadávací podmínky obsahovaly požadavky vytvářející překážky hospodářské soutěže, jestliže jsou objektivně zdůvodněny a jestliže jsou stanoveny v souladu se zásadami dle § 6 ZZVZ. Veřejní zadavatelé v tomto ohledu stojí před dvěma základními otázkami. Za prvé, jak objektivně zdůvodnit potřebu právě těch bezpečnostních opatření, jejichž požadavky zamýšlí promítnout do zadávacích podmínek. Za druhé, jak poznat míru nezbytnou pro jejich zohlednění v zadávacích podmínkách.

Vyhláška č. [82/2018](#) Sb., o kybernetické bezpečnosti (dále jen „VKB“), staví zavádění a provádění bezpečnostních opatření na konceptu řízených rizik. Právě kvalifikované hodnocení rizik a na něj navazující prohlášení o aplikovatelnosti zpracované dle VKB je objektivním základem pro požadavky, které je veřejný zadavatel povinen zakomponovat do zadávacích podmínek a které mohou vytvářet překážky hospodářské soutěže. Z týchž podkladů vyplyne cíl daného bezpečnostního opatření, které musí být ve vztahu k tomuto cíli přiměřené. Bezpečnostní opatření promítnuté do zadávacích podmínek, které by jinak působilo diskriminačně, tedy nesmí být excesivní, tj. nesmí přesahovat míru nezbytnou pro zvládnutí příslušných rizik (nesmí být „zbytečně silné“). Nesmí existovat žádné další rozumně dosažitelné bezpečnostní opatření sledující stejný cíl, které omezuje hospodářskou soutěž méně než zamýšlené bezpečnostní opatření.

Z výše uvedeného vyplývá, že nutnou podmínkou je pro veřejné zadavatele kvalifikované provedení hodnocení rizik a zpracování prohlášení o aplikovatelnosti, případně další dokumentace předepsané VKB. Tím veřejný zadavatel, při dodržení zásady přiměřenosti, dosáhne objektivizace svých bezpečnostních potřeb ve vztahu k předmětu dotčené veřejné zakázky. Tento závěr lze opřít o rozhodnutí Úřadu pro ochranu hospodářské soutěže (dále jen „ÚOHS“) ze dne 6. 11. 2019 č. ÚOHS-S0262/2019/VZ-30266/2019/523/JMa: „...sporné opatření je (s výjimkou úplného vyloučení řešení

dotčených společností) jediným opatřením pro zabránění nedostupnosti služby, které mohl zadavatel reálně přijmout. S ohledem na povinnosti zadavatele plynoucí ze ZKB by bez přijetí sporného opatření ani nemohl předmět veřejné zakázky poptávat. Zároveň Úřad (i v kontextu stanoviska NÚKIB) uzavřel, že se nejedná o podmínku jakkoliv excesivní. Její zařazení do zadávací dokumentace tak nepředstavuje libovůli zadavatele, nýbrž jediný způsob, jak mohl zadavatel dostat svým zákonným povinností v oblasti kybernetické bezpečnosti. Zadavatel je přitom povinen se při zadávání veřejných zakázek řídit právním řádem České republiky jako celkem. Nemůže-li tak zadavatel dodržet svou zákonnou povinnost při zadávání veřejné zakázky v oblasti kybernetické bezpečnosti jinak, než přijetím sporného opatření, nejedná se o nedovolenou diskriminaci, neboť takový závěr by vedl k situaci, kdy by zadavatel předmět veřejné zakázky vůbec nemohl poptat, a to bez jakéhokoliv zavinění z jeho strany.“ V řešeném případě zadavatel na základě provedeného hodnocení rizik, při kterém přihlédl k varování Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) ohledně výrobků některých čínských společností^[1], identifikoval potřebu vysoké dostupnosti poptávaného řešení a stanovil bezpečnostní opatření spočívající v redundanci některých zařízení pomocí zařízení nečínských výrobců. V zadávací dokumentaci k tomu zadavatel dle citovaného rozhodnutí ÚOHS uvedl: „Uvedeným opatřením, v případě dodávek řešení výrobců, před kterými varoval NÚKIB, je dodávka a zajištění stavu vysoké dostupnosti řešení – ke každému kusu dodaného hardware dodávka druhého kusu hardware od nečínského výrobce a jejich plná společná integrace tak, aby takové řešení plnilo funkci zajištění vysoké dostupnosti a současně i veškeré Zadavatelem definované požadavky v rámci zadávacích podmínek k Veřejné zakázce.“

Podle § 5 odst. 1 písm. h) VKB musí povinná osoba opatření dle § 11 ZKB, tj. i varování, zohlednit při hodnocení rizik, což se může projevit i nutností zahrnout do zadávacích podmínek požadavky, které by bez objektivizace skrze hodnocení rizik nebyly v souladu se ZZVZ. Hodnocení rizik musí povinná osoba provádět v pravidelných intervalech a vždy při významných změnách, které mohou mít vliv na kybernetickou bezpečnost chráněných systémů a představují vysoké riziko. Konstatuje-li NÚKIB existenci nějaké hrozby formou varování, jde nepochybně o skutečnost, na kterou by povinné osoby měly reagovat aktualizací hodnocení rizik.

Lze shrnout, že veřejní zadavatelé musí stanovit a provádět bezpečnostní opatření pro zajištění kybernetické bezpečnosti. Současně musí tato bezpečnostní opatření zohledňovat v zadávacích podmínkách. Požadavky vyplývající z bezpečnostních opatření musí být opřeny o objektivně provedené hodnocení rizik a musí být přiměřené sledovanému cíli. Hodnocení rizik musí být prováděno pravidelně a rovněž v reakci na významné změny. Současně by se mělo jednat o hospodárné řešení. Jak totiž dle citovaného rozhodnutí ÚOHS připomíná sám NÚKIB: „Nezbytnou součástí zvažování přiměřenosti bezpečnostního opatření [o které hovoří § 3 písm. c) VKB] je též posouzení hospodárnosti zvoleného postupu, zejm. tedy zda náklady spojené se zavedením bezpečnostního opatření nejsou neúměrné nákladům spojeným s realizací rizika.“



Mgr. Ing. Robert Kotzian, Ph.D.
Právník a bývalý programátor-analytik

E-mail: robert@kotzian.cz

[1] Varování NÚKIB ze dne 17. 12. 2018 č. j. 3012/2018-NÚKIB-E/110, ve kterém tento úřad na základě § 12 odst. 1 ZKB upozornil, že použití prostředků společností Huawei Technologies Co., Ltd. a ZTE Corporation, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti. K dispozici >>> [zde](#).

© EPRAVO.CZ - Sběrka zákonů, judikatura, právo | www.epravo.cz

Další články:

- [JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - KVĚTEN 2026](#)
- [Hodnocení demo prostředí v IT veřejných zakázkách: užitečný nástroj, nebo cesta k netransparentnosti?](#)
- [JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - DUBEN 2026](#)
- [Prokazování dostupnosti technického vybavení při zadávání veřejných zakázek - limity sdílení technického vybavení](#)
- [JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - BŘEZEN 2026](#)
- [Zdrojové kódy jako „pojistka“ proti vendor-lock-inu: judikatorní korekce a její meze](#)
- [Spolupráce zadavatele a developera z pohledu rozhodovací praxe ÚOHS a plánovacích smluv](#)
- [Listinné nabídky v éře elektronizace: přestupek, nebo legitimní postup?](#)
- [JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - ÚNOR 2026](#)
- [Změna poddodavatele v průběhu zadávacího řízení](#)
- [JIŘÍ HARNACH - VEŘEJNÉ ZAKÁZKY LIVE! - LEDEN 2026](#)