9. 11. 2020

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

IT bezpečnost při zadávání veřejných zakázek

Informační technologie jsou v současné době zahrnuty ve většině oblastí činnosti zadavatelů a jejich význam bude i nadále růst[1]. Spolu s rostoucím významem informačních technologií a informací v nich obsažených se zvyšují i nároky na jejich bezpečnost. Roste tedy počet zranitelností a s nimi i rizika, že dané zranitelnosti budou využity hrozbami, a dojde tak ke škodám na informačních aktivech[2] zadavatelů[3]. Základem IT bezpečnosti bez ohledu na postavení zadavatele tak vždy bude zajištění důvěrnosti, integrity a dostupnosti informačních aktiv.

K IT bezpečnosti se vztahuje celá řada právních přepisů[4], standardů a metodik, které společně vedou k ochraně informačních aktiv zadavatelů. V tomto článku se zaměříme pouze na jeden z mnoha aspektů této problematiky, a to na bezpečné poskytování informací při zadávání veřejných zakázek dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“).

Z pohledu ZZVZ se při ochraně informací ve vztahu k IT bezpečnosti střetávají dvě základní pravidla, a to potřebnost ochrany informací poskytovaných zadavatelem při zadávání veřejné zakázky a požadavek na transparentnost zadávání veřejné zakázky. Zadavatel proto bude muset vždy nejdříve uvážit, jaké informace dodavatelům bude nezbytné poskytnout (podrobnost nezbytná pro účast dodavatelů v zadávacím řízení) a zda takové informace je nutné z pohledu IT bezpečnosti chránit.

Jestliže pro řádný a se ZZVZ souladný postup při zadávání veřejné zakázky bude potřebné poskytnout informace, jež bude třeba chránit, měl by zadavatel uvážit nejvhodnější možnost ochrany. Vedle zcela specifické úpravy veřejných zakázek v oblasti bezpečnosti dle části deváté ZZVZ, která se uplatní zejména tam, kde se předmět veřejné zakázky dotýká utajovaných informací, budou pro zadavatele podstatná ustanovení § 36 odst. 8, § 96 odst. 2 a § 211 odst. 3 ZZVZ.

Dle § 96 odst. 2 ZZVZ může zadavatel příslušnou část zadávací dokumentace poskytnout jiným vhodným způsobem než uveřejněním zadávací dokumentace na profilu zadavatele, pokud takovou část zadávací dokumentace nelze uveřejnit z důvodů vymezených v § 211 odst. 3 písm. d) ZZVZ nebo v případě postupu podle § 36 odst. 8 ZZVZ.

V souladu s § 36 odst. 8 ZZVZ může zadavatel požadovat, aby dodavatel přijal přiměřená opatření k ochraně důvěrné povahy informací, které zadavatel poskytuje nebo zpřístupňuje v průběhu zadávacího řízení.

Dle § 211 odst. 3 písm. d) ZZVZ písemná komunikace mezi zadavatelem a dodavatelem nemusí probíhat elektronicky v případě, kdy použití jiné než elektronické komunikace je nezbytné z důvodu ochrany zvláště citlivé povahy informací, přičemž požadovanou úroveň zabezpečení nelze řádně zajistit běžně dostupnými elektronickými nástroji nebo nástroji podle § 103 odst. 3 ZZVZ.

Zadavatel tak nejčastěji bude poskytovat dodavatelům chráněné informace na základě dohody o mlčenlivosti nebo prohlášení o mlčenlivosti (dále jen „NDA“) [5]. Pro zachování řádné ochrany informací bude nezbytné, aby zadavatel dbal na precizní vymezení NDA, a to zejména na specifikaci informací, které podléhají ochraně; nakládání s těmito informacemi včetně hmotného podkladu, na kterém jsou zachyceny; okruh osob, které budou s informacemi oprávněny nakládat, včetně poddodavatelských vztahů; a formulaci sankcí za porušení povinností dodavatele. V této souvislosti je

třeba také zmínit, že i NDA představuje komunikaci zadavatele s dodavatelem dle § 211 odst. 1 ZZVZ, která by měla probíhat elektronicky.

Ve většině případů budou chráněné informace poskytnuty na hmotném podkladu[6] a zadavatel by měl zvážit zabezpečení i takového hmotného podkladu, a to jak proti zneužití, tak také pro potřeby identifikace dodavatele, kterému byl hmotný podklad poskytnut, v případě prokazování porušení NDA.

Jestliže zadavatel dospěje do fáze, kdy má vymezeno, jaké informační aktiva bude chránit (část zadávací dokumentace) a jaký zvolí způsob ochrany (poskytnutí na základě NDA), pak by si měl stanovit, kdy bude chráněná informace dodavatelům poskytnuta. S tímto posouzením souvisí zejména volba druhu zadávacího řízení.

Jestliže zadavatel zvolí vícefázové zadávací řízení, pak může v odůvodněných případech zvolit postupné poskytování chráněných informací v návaznosti na potřebnost informací pro účast dodavatele v příslušné fázi zadávacího řízení. Např. metodický materiál Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) s označením „ZADÁVÁNÍ VEŘEJNÝCH ZAKÁZEK V OBLASTI ICT A KYBERNETICKÁ BEZPEČNOST“[7] doporučuje pro ochranu informací využívat jednací řízení s uveřejněním.

V rámci jednacího řízení s uveřejněním může zadavatel poskytnout část chráněných informací ve lhůtě pro podání žádostí o účast a další část až dodavatelům, kteří prokázali splnění kvalifikace a byli vyzváni k podání předběžné nabídky, a to ve lhůtě pro podání předběžných nabídek. V odůvodněných případech bude možné poskytnout chráněné informace i na jednání o předběžné nabídce.

Jestliže se bude předmět veřejné zakázky vztahovat ke kybernetické bezpečnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZKB“), mohou zadavatelé pro potřeby ochrany informací využít také ustanovení § 4 odst. 4 ZKB, dle kterého jsou orgány a osoby uvedené v § 3 písm. c) až f) ZKB povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření dle výše uvedeného v míře nezbytné pro splnění povinností podle ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Vzhledem k tomu, že povinnost zveřejňování informací se váže nejenom k zahájení zadávacího řízení, ale také k jeho ukončení, měl by zadavatel při ochraně informací z pohledu IT bezpečnosti zvážit i problematiku uveřejňování výsledku zadávacího řízení (zejména uzavřené smlouvy) a poskytování informací o zadávacím řízení (např. dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů).

Dle § 3 odst. 1 zákona č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů se prostřednictvím registru smluv neuveřejňují informace, které nelze poskytnout při postupu podle předpisů upravujících svobodný přístup k informacím.

Dle § 11 odst. 1 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů povinný subjekt může omezit poskytnutí informace, pokud její poskytnutí významně nebo přímo ohrožuje účinnost bezpečnostního opatření stanoveného na základě zvláštního předpisu pro účel ochrany bezpečnosti osob, majetku a veřejného pořádku.

Pokud tedy zadavatel bude chránit informace, které jsou citlivé povahy a není žádoucí, aby vešly v

obecnou známost (opatření, které má svůj podklad v zákoně), bude zadavatel oprávněn tyto informace neuveřejnit nebo neposkytnout, a to i když se dle ZZVZ předpokládá jejich zpřístupnění (např. informace, jejichž zveřejnění by mohlo ohrozit kybernetickou bezpečnost).[8]

V neposlední řadě poskytuje zadavateli určité východisko k ochraně informací před povinným uveřejňováním i samotný ZZVZ v ustanovení § 218 odst. 3 ZZVZ, dle kterého zadavatel nemusí uveřejnit informaci podle ZZVZ, pokud by její uveřejnění znamenalo porušení jiného právního předpisu nebo by bylo v rozporu s veřejným zájmem, nebo by mohlo porušit právo dodavatele na ochranu obchodního tajemství nebo by mohlo ovlivnit hospodářskou soutěž.

I když to nemusí být na první pohled zřejmé, ZZVZ samostatně, či společně s jinými právními předpisy nabízí zadavateli rozličné možnosti, jak ochránit z pohledu IT bezpečnosti významná informační aktiva. Nicméně všechny způsoby ochrany budou odvislé od schopnosti zadavatele takové postupy nejen v praxi efektivně využít, ale také si jejich využití řádně odůvodnit. Zadavatel je ten, kdo nejlépe zná povahu a význam jím poskytovaných informací, a tedy právě on musí dodavatele a kontrolní orgány přesvědčit, že v konkrétním případě při ochraně informací nepostupuje netransparentně či snad diskriminačně a svévolně, ale že pouze aplikuje opatření nezbytná k zajištění IT bezpečnosti jeho informačních aktiv.

Pro řádné a se ZZVZ souladné zajištění IT bezpečnosti při zadávání veřejných zakázek lze zadavateli doporučit, aby tuto oblast nepodceňoval a neponechával ji pouze na nahodilých řešeních, ale aby si nastavil interní předpisy řešící tuto problematiku a sledoval aktuální věcné i právní výkladové tendence (např. Národní centrum kybernetické bezpečnosti, Národní CSIRT České republiky).

Mgr. Lenka Lelitovská,
advokátní koncipient

MT Legal s.r.o., advokátní kancelář

Jugoslávská 620/29
120 00 Praha 2

Tel.: +420 222 866 555
Fax: +420 222 866 546
e-mail: info@mt-legal.com

---

[1] Informace a informační procesy, které u zadavatelů probíhají, budou postupně digitalizovány např. i v souvislosti s dopady zákona č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů, ve znění pozdějších předpisů.

[2] Informační aktiva představují zejména zařízení, programy a informace, které jsou podstatné pro

výkon činností zadavatele.

[3] Např. Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 uvádí následující: „Pokračující digitalizace veřejné správy v České republice slouží k zlepšení fungování veřejné správy a jejího vztahu k veřejnosti. Avšak služby a aplikace poskytované občanům a soukromým podnikům prostřednictvím eGovernment s sebou nesou značná kybernetická bezpečnostní rizika.“

[4] Zejména zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů; zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů a zákon č. 110/2019 Sb., o zpracování osobních údajů.

[5] non-disclosure agreement

[6] Výjimkou budou situace, kdy zadavatel bude poskytovat chráněné informace pouze k nahlédnutí (např. zdrojové kódy informačního systému).

[7] Verze metodického materiálu 1.3, platná ke dni 30. 7. 2020, dk dispozici >>> zde.

[8] Podpůrným materiálem pro zadavatele v této souvislosti může být Doporučení k (ne)poskytování informací v oblasti kybernetické bezpečnosti a bezpečnosti systémů nakládajících s utajovanými informacemi zpracované NÚKIB, verze 2.0, platná ke dni 24. 8. 2020 a k dispozici >>> zde.

Další články:

- 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
- Metoda Design & Build na poli veřejných zakázek
- Požadavek zadavatele na prokazování referencí prostřednictvím staveb občanské vybavenosti ve světle rozhodovací praxe