NÚKIB

ZOHLEDNĚNÍ VAROVÁNÍ ZE DNE 17. PROSINCE 2018 V ZADÁVACÍM ŘÍZENÍ

Podpůrný materiál

Verze 1.1, platná ke dni 7. 1. 2022

Obsah

Úvod a cíl materiálu

Národní úřad pro kybernetickou a informační bezpečnost (dále též jen „NÚKIB“) vydal dne 17. prosince 2018 varování před použitím technických a programových prostředků (dále jen „prostředky“) společností Huawei Technologies Co., Ltd., a ZTE Corporation (č. j. dokumentu: 3012/2018-NÚKIB-E/110, dále jen „varování“).

Cílem tohoto materiálu je shrnout a akcentovat některé problémy, které NÚKIB do dnešního dne identifikoval v souvislosti s vydáním varování, a poskytnout **povinným osobám podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti** (dále jen „zákon o kybernetické bezpečnosti“ nebo „ZKB“), **které jsou současně zadavateli ve smyslu zákona č. 134/2016 Sb., o zadávání veřejných zakázek** (dále jen „zákon o zadávání veřejných zakázek“ nebo „ZZVZ“), metodickou pomoc při zohlednění varování při zadávání veřejných zakázek podle ZZVZ.

NÚKIB si je vědom toho, že problematika zadávání veřejných zakázek nespadá do jeho věcné působnosti, a tedy že není orgánem příslušným k závaznému výkladu ustanovení ZZVZ. Právní úprava zadávání veřejných zakázek však zasahuje i do oblasti kybernetické a informační bezpečnosti a úzce souvisí s povinnostmi osob spadajících do působnosti ZKB. Z toho důvodu považuje NÚKIB za nezbytné vyjádřit alespoň v této podpůrné rovině své stanovisko a napomoci tím zadavatelům při řešení problémů, kterým při zakomponování varování do svých bezpečnostních politik a při výběru dodavatelů svých informačních a komunikačních systémů mohou čelit.

Tímto stanoviskem NÚKIB však není a nemůže být dotčena odpovědnost zadavatelů za zákonnost zadávacího řízení, v němž bude zohledněno varování a v němž může dojít, s odkazem na plnění povinností podle ZKB, k omezení hospodářské soutěže.

Současně tímto stanoviskem NÚKIB nijak nenavádí zadavatele ke konkrétnímu postupu, který mají ve vztahu k zajištění kybernetické bezpečnosti svých informačních a komunikačních systémů aplikovat. Zohlednění informací obsažených ve varování ve svých strukturách je úkolem zadavatele, který si sám musí být nejlépe vědom specifik jím spravovaných či provozovaných informačních a komunikačních systémů a rizik, která jsou s jejich správou a provozováním spojena. Zákon o kybernetické bezpečnosti a na něj navazující podzákonné předpisy umožňují povinným osobám zvolit takový postup, který nejlépe vyhovuje jejich potřebám. Je tedy výlučně na odpovědnosti zadavatele, jakou úroveň kybernetické bezpečnosti bude aplikovat ve vztahu k jím spravovaným (resp. provozovaným) informačním a komunikačním systémům a jaká rizika bude ochoten akceptovat, a je to také zadavatel, kdo bude čelit případným důsledkům vyplývajícím z jím aplikovaného přístupu.

Obsah tohoto stanoviska byl konzultován s Ministerstvem pro místní rozvoj (gestorem zákona o zadávání veřejných zakázek).

V případě dotazů k tomuto dokumentu se prosím obracejte na sekretariát odboru regulace NÚKIB:

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 Manažerské shrnutí

Jak zákon regulující kybernetickou bezpečnost (ZKB), tak zákon regulující zadávání veřejných zakázek (ZZVZ) jsou předpisy stejné právní síly, nenacházejí se v žádném stavu nadřízenosti či podřízenosti, oba právní předpisy obecně nejsou v rozporu a orgány a osoby, které současně spadají do působnosti obou zákonů (dále též jen „zadavatelé“), jsou při výkonu své působnosti povinny postupovat tak, aby dostály požadavkům obou předpisů. Zákon o kybernetické bezpečnosti po povinných osobách mj. požaduje, aby zaváděly a prováděly bezpečnostní opatření za účelem zajištění kybernetické bezpečnosti informačních a komunikačních systémů. Zákon o zadávání veřejných zakázek vyžaduje, aby všechny požadavky omezující hospodářskou soutěž, které mají zadavatelé buďto na osobu dodavatele, nebo na předmět plnění veřejné zakázky, byly racionálně odůvodněny.

Varování označilo použití technických a programových prostředků vybraných dodavatelů za hrozbu v oblasti kybernetické bezpečnosti. Zákon o kybernetické bezpečnosti ani ZZVZ nestanoví automatickou povinnost zakázat v návaznosti na varování používání takto označených prostředků ve strukturách zadavatelů a v zadávacích řízeních. Zadavatelé si sami musejí vyhodnotit, zda použití uvedených prostředků v jejich systémech představuje riziko, které je třeba (zcela či částečně) eliminovat. Stěžejním dokumentem pro takové hodnocení je analýza rizik (která je součástí procesu hodnocení rizik), jejíž výsledky determinují navazující postup zadavatele při výběru konkrétních bezpečnostních opatření ke zvládání rizika.

Výsledky hodnocení rizik a výběr konkrétních bezpečnostních opatření pak determinují i znění zadávacích podmínek (za předpokladu, že se zadavatel rozhodne zjištěná rizika neakceptovat). Lze pak identifikovat dvě základní varianty postupu zadavatele – 1. hodnocení rizik a výběr bezpečnostních opatření provede zadavatel před zahájením zadávacího řízení, výsledné požadavky zanese do zadávací dokumentace a výběr dodavatele provede v otevřeném nebo užším řízení (příp. zjednodušeném podlimitním řízení), nebo 2. zadavatel stanoví iniciační zadávací podmínky a zahájí jednací řízení s uveřejněním, hodnocení rizik a výběr bezpečnostních opatření provede až v průběhu řízení, podle výsledků procesu hodnocení rizik a výběru bezpečnostních opatření případně upraví zadávací podmínky a po ukončení jednání na základě upravených zadávacích podmínek vybere ekonomicky nejvýhodnější nabídku.

Myšlenkové pochody zadavatele a jeho jednotlivé kroky při hodnocení rizik a při výběru bezpečnostních opatření by měly být dokumentovány, a to minimálně v rozsahu stanoveném v ZKB a jeho prováděcích předpisech a způsobem vyhovujícím požadavkům ZZVZ (především zásadě transparentnosti). Samotná analýza rizik nemusí být součástí zadávací dokumentace, její výsledky jsou podstatné pro posouzení odůvodnění nezbytnosti bezpečnostních opatření, které se do zadávací dokumentace promítly.

2 Základní východiska

Zákon o zadávání veřejných zakázek i ZKB jsou zákonnými předpisy stejné právní síly, nenacházejí se v žádném stavu nadřízenosti či podřízenosti, oba právní předpisy obecně nejsou v rozporu a orgány a osoby, které současně spadají do působnosti obou zákonů, jsou při své činnosti povinny postupovat tak, aby dostáli oběma právním předpisům.

Ze ZZVZ i ZKB zadavatelům plynou určité povinnosti. V případě ZZVZ jde zejm. o povinnost mít veškeré požadavky omezující hospodářskou soutěž racionálně odůvodněny (§ 36 odst. 1 ZZVZ), v případě ZKB jde o povinnost provádět bezpečnostní opatření za účelem zajištění kybernetické bezpečnosti informačních a komunikačních systémů a požadavky vyplývající z přijatých bezpečnostních opatření zanášet do smluv s dodavateli (§ 4 ZKB). Jedním z bezpečnostních opatření je řízení rizik [§ 5 odst. 2 písm. b) ZKB]. Podrobnosti k řízení rizik stanoví prováděcí právní předpis – 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 „vyhláška o kybernetické bezpečnosti“ nebo „VKB“). Při řízení rizik se provádí hodnocení rizik (čímž je myšlen celkový proces identifikace, analýzy a vyhodnocení rizik), v rámci kterého je zadavatel povinen zohlednit opatření NÚKIB vydaná podle § 11 ZKB, tedy i varování [§ 5 odst. 1 písm. h) bod 3. VKB].

Hodnocení rizik se provádí jednak v pravidelných intervalech a při významných změnách ve vztahu k aktivům existujících informačních nebo komunikačních systémů povinné osoby [§ 5 VKB a § 8 odst. 2 písm. c) VKB], jednak u významných dodavatelů ve vztahu k plnění poptávanému ve výběrovém řízení, a to v rámci tohoto výběrového řízení [§ 8 odst. 2 písm. a) VKB]. Dále se pak řízení rizik provádí ve vztahu k rizikům spojeným s dodavateli [§ 8 odst. 1 písm. e) VKB] a také v souvislosti s plánovanou akvizicí, vývojem a údržbou informačního a komunikačního systému [§ 13 písm. a) VKB]. Zákon o kybernetické bezpečnosti pak stanoví, že zohlednění požadavků vyplývajících z bezpečnostních opatření v míře nezbytné pro splnění povinností podle ZKB při výběru dodavatele nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži (§ 4 odst. 4 věta druhá a § 4 odst. 7 ZKB).

Stejně jako v případě povinností vyplývajících z dalších právních předpisů, které jsou zadavatelé v jednotlivých případech povinni dodržovat, i zde platí, že zadavatel zanese do zadávacích podmínek takové požadavky, kterými dostojí svým povinnostem vyplývajícím ze ZKB. Zadávací podmínky přitom budou reflektovat výsledky procesu hodnocení rizik, zejm. budou obsahovat konkrétní bezpečnostní opatření, která zadavatel zvolí pro snížení rizik, která identifikuje, na akceptovatelnou úroveň.

3 Zohlednění varování podle pravidel ZKB

Varování podle § 12 ZKB jsou orgány a osoby spadající do působnosti ZKB povinny zohlednit v procesu hodnocení rizik. Hodnocení rizik se provádí jednak ve vztahu k již zavedeným aktivům, jednak ve vztahu k aktivům, která povinná osoba do svých struktur teprve zavede po jejich nákupu. Z povahy věci se bude podoba standardního hodnocení rizik a tzv. předsmluvního hodnocení rizik [§ 8 odst. 2 písm. a) VKB] lišit – odlišný může být jednak rozsah posuzovaných aktiv, jednak i úroveň znalosti aktiv a hrozeb, které na ně mohou působit. Pro všechny případy však platí, že povinná osoba provádí hodnocení rizik v souladu s pravidly stanovenými bezpečnostní dokumentací a bezpečnostní politikou.

Varování (a ani ZKB) neukládá zadavatelům povinnost automaticky zakázat ve svých strukturách a v rámci zadávacích řízení použití prostředků společností Huawei Technologies Co., Ltd., ZTE Corporation a jejich dceřiných společností (dále jen „dotčené společnosti“). Zákon o kybernetické bezpečnosti však ukládá povinným subjektům povinnost zabývat se hrozbou, na kterou varování upozorňuje, a zvážit, zda a jaká bezpečnostní opatření je v konkrétních případech třeba přijmout. S takto identifikovanou hrozbou je třeba zacházet stejně jako se všemi ostatními hrozbami ve smyslu § 2 písm. e) VKB, které zadavatel standardně v souladu s § 5 odst. 1 písm. b) VKB identifikuje a v rámci hodnocení rizik dále zvažuje (s výjimkou toho, že hodnotu této konkrétní hrozby zde neurčuje sám zadavatel, ale NÚKIB). Riziko spojené s používáním prostředků dotčených společností může být na různých úrovních systémů různé, teprve analýza rizik zadavateli určí, na jakých místech a v jaké míře je potřeba na riziko reagovat.

Analýza rizik, která slouží jako podklad pro výběr konkrétních bezpečnostních opatření, musí být provedena tak, aby z ní bylo zřejmé, jakým způsobem jsou hodnocena rizika pro prostředky dotčených společností a jak jsou hodnocena rizika pro prostředky všech zbývajících výrobců působících na relevantním trhu[1]. Právě na tomto porovnání bude založen případný závěr o tom, že použití prostředků dotčených společností představuje v konkrétním případě samo o sobě riziko. Bezpečnostní dokumentace pak stanoví, zda a jakým způsobem je potřeba na zjištěné riziko reagovat.

Pokud riziko spojené s použitím prostředků dotčených společností přesáhne akceptovatelnou úroveň, snížení hodnoty rizika na akceptovatelnou úroveň je možné dvěma způsoby – 1. přijetím jiných (mírnějších) bezpečnostních opatření (pokud je to objektivně možné), nebo 2. úplným odstraněním prostředků dotčených společností ze struktur systému/systémů zadavatele (nebo jejich nevyužití, pokud ve struktuře systému/systémů dosud nejsou

[1] Hodnocení rizik ve vztahu k ostatním výrobcům bude odpovídat hodnocení rizik provedenému podle standardních pravidel zadavatele uplatňovaných do okamžiku vydání varování (tedy jako by varování vůbec nebylo vydáno). Tato pravidla mohou být v čase měněna (orgány a osoby spadající do působnosti ZKB jsou povinny své postupy revidovat a aktualizovat), vždy však má být zachována jejich univerzální použitelnost.

implementovány), pokud by jakékoli mírnější bezpečnostní opatření nebylo efektivní (nebo by bylo nepřiměřené).

Zadavatelé jsou přitom povinni reagovat na to, co je jim známo. Národní úřad pro kybernetickou a informační bezpečnost jako ústřední správní úřad pro oblast kybernetické bezpečnosti varováním označil používání prostředků dotčených společností za hrozbu v oblasti kybernetické bezpečnosti. Učinil tak na základě informací a podkladů, které v průběhu času nashromáždil a vyhodnotil. Tyto informace a podklady jsou z velké části vedeny v režimu utajovaných informací (ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti), z toho důvodu není možné je uveřejnit. Národní úřad pro kybernetickou a informační bezpečnost však po jejich přezkoumání dospěl k závěru, že faktický záběr hrozby je natolik široký, že není vhodné ji definovat ve větších podrobnostech, než jak to učinil ve varování. S ohledem na vymezení zákonných pravomocí NÚKIB v této oblasti pak není úkolem zadavatelů (resp. subjektů spadajících do působnosti ZKB obecně) přezkoumávat či rozporovat závěry NÚKIB, naopak je jejich povinností se těmito závěry řídit.

Varování označuje za hrozbu použití prostředků dotčených společností obecně. S ohledem na specifika jednotlivých informačních a komunikačních systémů spadajících pod ZKB a odlišné potřeby jednotlivých zadavatelů však není vyloučeno, aby zadavatelé na základě svých zkušeností a na svou odpovědnost extrahovali z obsahu varování, příp. z metodiky k varování vydané dne 4. ledna 2019 (dále jen „metodika k varování“), která stanoví demonstrativní výčet projevů varováním definované hrozby, určité typové hrozby (resp. projevy hrozby) a s těmi dále pracovali.

Ať již zadavatel postupuje jakýmkoli způsobem (tedy zohlední hrozbu jako celek, nebo pracuje s typovými hrozbami), obecně platí, že pokud výsledná hodnota zjištěného rizika přesahuje zadavatelem stanovené kritérium pro akceptovatelnost, zadavatel zváží přijetí efektivních bezpečnostních opatření. Naopak pokud hodnota rizika nepřekročí zadavatelem stanovenou hranici, není z pohledu ZKB a VKB nezbytné na takové riziko dále reagovat (bezpečnostní politika a bezpečnostní dokumentace však mohou stanovit speciální postup i pro tyto případy).

Záleží pak na hodnocení zadavatele, jaká konkrétní bezpečnostní opatření přicházejí za dané situace ke snížení neakceptovatelného rizika v úvahu a zda je ve vztahu ke konkrétnímu riziku schopen určit nějaká „mírnější“ bezpečnostní opatření (tj. jiná než úplný zákaz používání prostředků dotčených společností), která budou způsobilá riziko účinně eliminovat nebo alespoň snížit na akceptovatelnou úroveň.

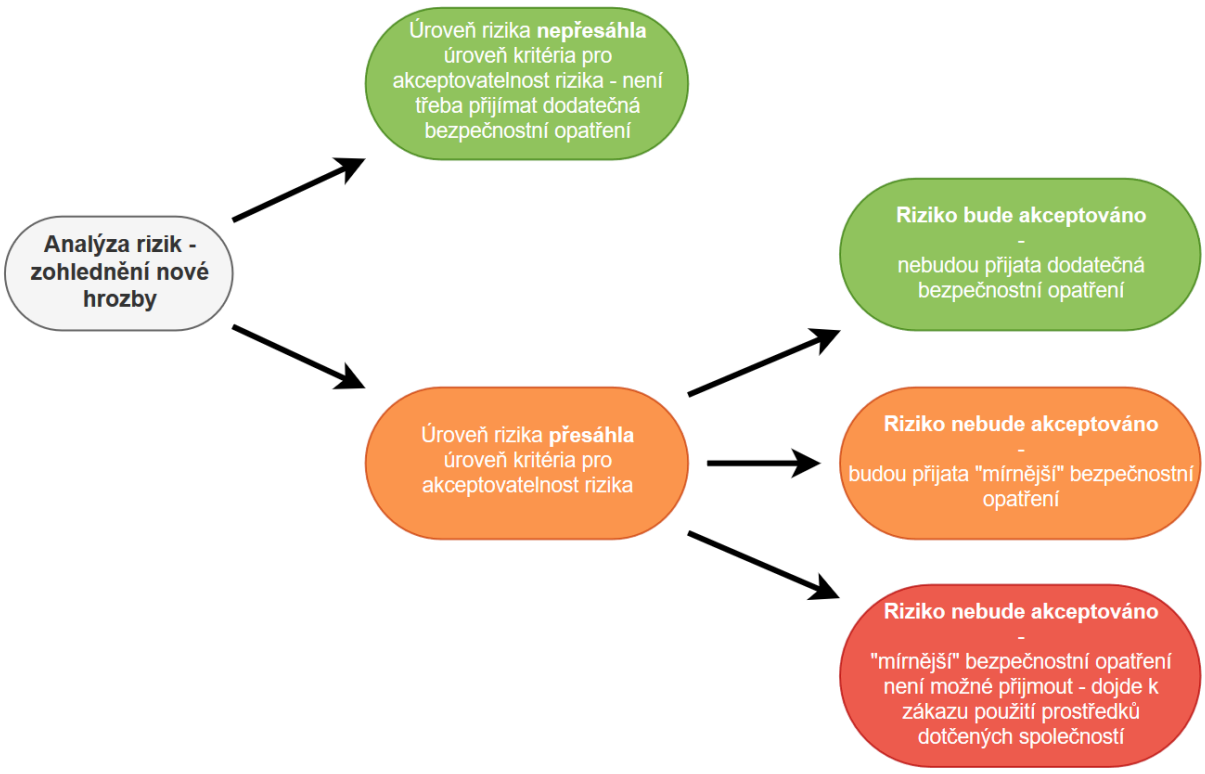
Pravidla pro určení neakceptovatelného rizika a pro volbu postupu v případě zjištění neakceptovatelného rizika, včetně obvykle používaného postupu pro eliminaci neakceptovatelného rizika, má mít zadavatel povinně podle požadavků ZKB obsaženu v bezpečnostní politice, resp. bezpečnostní dokumentaci (srov. zejm. přílohu č. 5 k VKB). Konkrétní postup zadavatele by tedy měl vycházet z těchto dokumentů. Není však vyloučeno,

aby zadavatel na základě této pro něho nové situace obecné postupy aktualizoval nebo doplnil o nová pravidla, která bude do budoucna v obdobných situacích aplikovat.

Současně je třeba mít na paměti, že v případě hodnocení rizika je takové riziko závislé nejen na úrovni hrozby, ale také na úrovni zranitelnosti a dopadu, kdy je určitým rizikem (tedy jeho hodnotou) chápána kombinace uvedených veličin (VKB pracuje se vzorcem *riziko = dopad * hrozba * zranitelnost*). I v případě, kdy je hrozba hodnocena jako kritická, tedy může být výsledné riziko hodnoceno např. jako nízké, protože zranitelnost a dopad kritických hodnot dosahovat nebudou (viz příloha č. 2 VKB s tabulkami úrovní). V takovém případě pak nemusí nastat důvod pro eliminaci hrozby spojené s využitím prostředků dotčených společností, protože výsledné identifikované riziko nepřesáhne hodnotu kritéria pro akceptovatelnost rizika, kterou má zadavatel stanovenu v souladu s požadavky § 5 VKB, a zadavatel v reakci na hrozbu nebude muset přijímat žádná dodatečná bezpečnostní opatření.

Současně není vyloučeno, aby si zadavatel ve svých bezpečnostních politikách stanovil mechanismus pro zvážení a případnou akceptaci rizika, jehož hodnota přesahuje stanovené kritérium pro akceptovatelnost. Takový postup však musí být rozumně odůvodněn a měl by být aplikován pouze výjimečně.

Výše popsaný postup shrnuje následující schéma:



Obrázek 1: Schéma postupu zadavatele při hodnocení rizik ve světle nové hrozby

4 Stanovení typových hrozeb

Jak již bylo uvedeno výše, varování označuje za hrozbu použití prostředků dotčených společností bez další konkretizace. Obecně však není vyloučeno, aby zadavatelé na základě svých zkušeností a na svou odpovědnost extrahovali z obsahu varování nebo metodiky k varování určité typové hrozby (*de facto* konkrétní projevy varováním definované hrozby) a s těmi dále pracovali. Není totiž *a priori* v rozporu se ZKB nebo VKB, pokud zadavatel v analýze rizik stanovením typových hrozeb navázaných na prostředky dotčených společností zohlední *de facto* pouze určitou množinu projevů hrozby, na kterou varování upozorňuje (na principu výběru relevantních proměnných, tedy i hrozeb, je ostatně založen celý systém řízení bezpečnosti informací včleněný do VKB).

Pro řádné zohlednění varování v analýze rizik je však třeba typové hrozby hodnotit jak ve vztahu k prostředkům dotčených společností, tak ve vztahu k prostředkům ostatních výrobců.

Stejně tak je potřeba hodnotit hrozbu (ať již definovanou obecně, nebo pomocí konkrétních projevů) takovou hodnotou, jakou stanovil NÚKIB ve varování.

Zadavatelé tedy nejsou za všech okolností povinni definovat hrozbu (nikoli však její hodnotu) jednotným způsobem. Záležet bude především na úrovni znalosti plnění, které je v rámci konkrétní veřejné zakázky poptáváno.

Pokud zadavatelé poptávají plnění, o jehož technické stránce (provedení) mají relativně podrobné informace (např. jsou schopni sami v podrobnostech nadefinovat technické provedení poptávaného plnění), nebo jde o relativně sourodé a jednoduché plnění (např. servery, notebooky), budou obecně schopni nadefinovat i konkrétnější podobu hrozby navázané na použití prostředků dotčených společností. Pokud mají zadavatelé s určitým plněním zkušenosti (nebo jsou s technickými podrobnostmi plnění obeznámeni z jiného důvodu), jsou nepochybně obeznámeni i se zranitelnostmi, které takové plnění standardně má, a hrozbami, které na něj obvykle působí. Mohou tedy na základě svých zkušeností určit, jaké konkrétní hrozby jsou relevantní ve vztahu k jakému aktivu, a takové hrozby pak z varování extrahují.

Naopak pokud budou zadavatelé poptávat plnění, o jehož technické stránce mají pouze omezené informace (např. předmětem veřejné zakázky bude informační systém, u něhož si zadavatel nadefinoval pouze požadavky na funkčnost a základní parametry, avšak konkrétní technické řešení ponechal na dodavateli), budou jejich možnosti při stanovení konkrétních hrozeb navázaných na použití prostředků dotčených společností omezené. V takovém případě bude zadavatel spíše schopen zohlednit pouze obecnou hrozbu použití prostředků dotčených společností (bez další konkretizace) a porovnat ji se zranitelnostmi aktiv, které v okamžiku tvorby analýzy rizik zná.

Obecně tedy lze doporučit, aby zadavatelé volili konkrétní postup zohlednění hrozby v analýze rizik podle charakteru poptávaného plnění a podle míry informací, kterými o poptávaném plnění disponují. Platí přitom, že čím více informací o technických specifikách poptávaného

plnění zadavatel má, tím podrobněji je schopen nadefinovat zranitelnosti a hrozby, které mohou na jednotlivá aktiva působit. Současně je žádoucí se při formulaci hrozeb soustředit na všechny tři atributy bezpečnosti informací, tedy dostupnost, důvěrnost a integritu.

5 Výběr konkrétních bezpečnostních opatření

Ustanovení § 4 odst. 2 ZKB stanoví, že orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření **v rozsahu nezbytném pro zajištění kybernetické bezpečnosti** informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému.

Druhá věta § 4 odst. 4 (obdobně odst. 7) ZKB stanoví, že zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první **v míře nezbytné pro splnění povinností podle tohoto zákona** nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Pro poskytovatele digitální služby platí, že jsou povinni zavést a provádět **vhodná a přiměřená** bezpečnostní opatření pro sítě elektronických komunikací a informační systémy (§ 4 odst. 3 ZKB).

Pro orgány a osoby uvedené v § 3 písm. c) až g) ZKB, které jsou orgány veřejné moci, platí, že jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu **stanovená NÚKIB** (§ 4 odst. 5 ZKB).

Vyhláška o kybernetické bezpečnosti v § 3 mj. stanoví, že povinná osoba v rámci systému řízení bezpečnosti informací (…) pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik **zavede přiměřená bezpečnostní opatření**. Uvedené v praxi znamená především to, že náklady na bezpečnostní opatření by měly být vždy přiměřené a neměly by převýšit náklady spojené s následky realizace rizika (viz metodika k varování). Současně platí, že by neměla být zaváděna bezpečnostní opatření proti neexistujícím rizikům.

5.1 Proces vyhodnocení rizika

Ve vztahu k zadávacímu řízení na dodávku technických nebo programových prostředků (poptávaných nikoli nutně samostatně) ve světle vydaného varování lze identifikovat čtyři základní situace, ve kterých se mohou zadavatelé po provedení analýzy rizik nebo aktualizaci jejích hodnot ocitnout:

1. Identifikovaná hodnota rizika nepřesáhne úroveň kritéria pro akceptovatelnost rizika, které má zadavatel stanoveno v souladu s požadavky § 5 VKB, zadavatel tedy nemusí přijímat dodatečná bezpečnostní opatření, která by byl v souladu s § 4 odst. 4 nebo 7 ZKB povinen zohlednit v zadávacím řízení.
2. Identifikovaná hodnota rizika přesáhne úroveň kritéria pro akceptovatelnost rizika, které má zadavatel stanoveno v souladu s požadavky § 5 VKB, zadavatel je tedy povinen zvážit svůj další postup a případně přijmout bezpečnostní opatření podle § 4 ZKB a požadavky vyplývající z bezpečnostních opatření v souladu s § 4 odst. 4, 5 anebo 7 ZKB zohlednit

v zadávacím řízení. Konkrétní postup, resp. bezpečnostní opatření vedoucí ke snížení rizika, přitom zadavatel volí na základě výsledků analýzy rizik podle konkrétních podmínek fungování jeho informačních a komunikačních systémů, při zohlednění bezpečnostních politik a pravidel stanovených v bezpečnostní dokumentaci a přiměřenosti, včetně nákladů, které mu v souvislosti s přijetím bezpečnostních opatření vzniknou. Zadavatel přitom může dospět k těmto závěrům:

a) Riziko spojené s používáním prostředků dotčených společností bude i přes překročení hranice stanovené pro akceptaci rizika akceptováno, a to s rozumným odůvodněním (např. přijetí adekvátního bezpečnostního opatření by bylo nepřiměřeně drahé, nasazení adekvátního bezpečnostního opatření není z technických důvodů možné apod.).

b) Ke snížení rizika spojeného s používáním prostředků dotčených společností na akceptovatelnou úroveň není třeba tyto prostředky zakazovat v zadávacím řízení úplně. Bezpečnostní opatření přijatá na základě § 4 ZKB mohou spočívat např. v doplnění prostředků dotčených společností prostředky jiných společností nebo v přijetí jiných opatření (a to jak na straně zadavatele, tak na straně dodavatele), která zajistí snížení hodnoty rizika za současného zachování možnosti používat prostředky dotčených společností. Pokud by zadavatel přistoupil k přijetí “přísnějšího" bezpečnostního opatření a takové řešení požadoval v zadávací dokumentaci, nebylo by možné hovořit o přijetí opatření v míře nezbytné pro splnění povinností podle ZKB a přijatá opatření by tak nebylo možné automaticky bez dalšího hodnotit jako zákonná omezení hospodářské soutěže nebo odůvodněnou překážku hospodářské soutěže.

c) Snížení rizika spojeného s používáním prostředků dotčených společností na akceptovatelnou úroveň nelze dosáhnout jinak než úplným zákazem používání prostředků dotčených společností v informačních a komunikačních systémech zadavatele, a tím i zákazem těchto prostředků v zadávacím řízení, případně zavedením nepřiměřených (zejm. přehnaně nákladných) bezpečnostních opatření (pokud taková vůbec existují). Zákaz prostředků dotčených společností je tak ve světle ZKB jediným v úvahu přicházejícím opatřením zajišťujícím snížení rizika spojeného s užíváním prostředků dotčených společností. Stanovení zadávacích podmínek v tom smyslu, že zadavatel nebude akceptovat nabídky dodavatelů, kteří nabídnou řešení založené na/obsahující prostředky dotčených společností, pak bude naplňovat hypotézu druhé věty § 4 odst. 4 nebo § 4 odst. 7 ZKB a nebude představovat nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěže.

5.2 Hodnocení přiměřenosti bezpečnostních opatření

Přiměřenost je neurčitý právní pojem, jehož definice není jednotná a jehož obsah je třeba posuzovat ve vztahu ke konkrétním skutkovým okolnostem. Např. Strategie pro oblast

kybernetické bezpečnosti České republiky na období 2012-2015[2] stanoví: „*Při zajištění kybernetické bezpečnosti nelze dosáhnout absolutní bezpečnosti. V České republice budou přijímána taková opatření, která budou založena na realistickém ohodnocení rizika a budou adekvátní těmto rizikům. Tato opatření budou respektovat ochranu soukromí a základní práva, jako je svobodný přístup k informacím, svoboda vyjadřování a další. Bude zajištěna přiměřenost přijatých opatření vzhledem k nutnosti zajistit bezpečnost na jedné straně a respektování základních práv a svobod na straně druhé*.“ Posouzení nepřiměřenosti nákladů na přijetí bezpečnostních opatření se věnuje i metodický materiál NÚKIB[3]. Přiměřenost je však třeba posuzovat nejen ve vztahu k finanční hodnotě přijatých opatření, ale též ve vztahu k nefinančním skutečnostem (charakter informačního nebo komunikačního systému, předmět činnosti povinného subjektu, ochrana práv třetích osob, zajištění otevřené soutěže apod.).

Obecně pak platí, že ne všechna reálně proveditelná bezpečnostní opatření vedoucí k zajištění kybernetické bezpečnosti jsou ve vztahu ke konkrétnímu informačnímu nebo komunikačnímu systému za konkrétních skutkových okolností přiměřená.

Přiměřenost bude nezbytné posuzovat ve vztahu ke všem bezpečnostním opatřením, která bude zadavatel v dané chvíli objektivně schopen přijmout (v praxi se bude zadavatel zejm. rozhodovat mezi zákazem použití prostředků dotčených společností, přijetím jiných bezpečnostních opatření a akceptací rizika).

Hodnocení přiměřenosti konkrétních bezpečnostních opatření bude záviset na konkrétních skutkových okolnostech – zejm. charakteru a důležitosti informačního nebo komunikačního systému, charakteru a důležitosti informací zpracovávaných zadavatelem prostřednictvím jeho informačních nebo komunikačních systémů, absolutní i relativní výši nákladů na zavedení „mírnějších“ bezpečnostních opatření (zejm. ve vztahu k nákladům spojeným s následky realizace rizika nebo nákladům na pořízení celého informačního nebo komunikačního systému), počtu subjektů operujících na relevantním trhu (otevřenost soutěže), časovém hledisku implementace „mírnějších“ bezpečnostních opatření, potenciálních nefinančních následcích při akceptaci rizika souvisejícího s používáním prostředků dotčených společností apod.

Do přiměřenosti z hlediska ZKB (resp. VKB) pak vstupuje i hodnocení přiměřenosti z hlediska ZZVZ (srov. § 6 odst. 1 ZZVZ).[4] Pokud je však dodržen požadavek na přiměřenost definovaný v ZKB (resp. VKB), za současného dodržení dalších podmínek definovaných těmito předpisy,

[2] https://www.govcert.cz/download/legislativa/container-nodeid-719/20120209strategieprooblastkbnbu.pdf
[3] https://www.govcert.cz/download/kii-vis/obecne/Neprimerene-naklady_v2.1.pdf
[4] Způsob provedení posouzení přiměřenosti konkrétního požadavku zadavatele je popsán např. v rozhodnutí Úřadu pro ochranu hospodářské soutěže ze dne 16. 10. 2013, č. j. ÚOHS-S262/2013/VZ-20122/2013/521/GSt, a to následovně: „*Samotná proporcionalita se poměřuje naplněním tří dílčích kritérií, které představuje vhodnost, potřebnost a proporcionalita v užším slova smyslu (tzv. test proporcionality). V posuzování vhodnosti opatření se zkoumá, zda opatření vede k účelu, který má naplňovat. Kritérium potřebnosti určuje, zda nelze dosáhnout požadovaného účelu i jiným prostředkem, než je poměřované opatření. Posledním kritériem je proporcionalita v užším slova smyslu, tedy poměřování toho, zda je posuzované opatření skutečně přiměřené požadovanému cíli a nepředstavuje exces či neúnosné narušení některého ze základních principů zákona o veřejných zakázkách.*“

presumuje se (viz § 4 odst. 4 ZKB), že takový požadavek vyhovuje ustanovení § 36 odst. 1 ZZVZ, kterým jsou základní zásady obsažené v § 6 odst. 1 a 2 ZZVZ, tedy i zásada přiměřenosti, ve vztahu k tvorbě zadávacích podmínek rozvedeny (mělo by být tedy presumováno i dodržení zásady přiměřenosti podle ZZVZ). Při zvažování přiměřenosti konkrétního opatření by měly být brány v potaz srovnatelné proměnné. V praxi by proto nemělo docházet k situacím, kdy bude konkrétní bezpečnostní opatření hodnoceno z hlediska ZKB jako přiměřené, zatímco z hlediska ZZVZ nikoli.

5.3 Náklady na zavedení bezpečnostních opatření

Povinnými osobami podle ZKB (a tedy osobami odpovědnými za dodržení povinností vyplývajících z tohoto zákona) jsou správce informačního nebo komunikačního systému (v pozici zadavatele) a současně jeho provozovatel (v pozici dodavatele). Zákon o kybernetické bezpečnosti ani ZZVZ však nestanoví, jakým způsobem mají být hrazeny náklady související se zavedením bezpečnostních opatření. Distribuce nákladů na zabezpečení informačních a komunikačních systémů tak bude předmětem dohody mezi těmito osobami.

V případě zadávacího řízení bude rozhodující znění zadávacích podmínek, ze kterých by mělo jasně vyplývat vymezení povinností dodavatele a požadavků zadavatele na způsob stanovení nabídkové ceny (tj. která bezpečnostní opatření jsou zahrnuta v nabídkové ceně).

6 Postup v případě, že je poptáván nový systém, u něhož v zadávací dokumentaci nejsou definovány všechny technické specifikace (tzn. podoba výsledného řešení je částečně v dispozici dodavatele)

Pozn.: Následující text popisuje vybrané situace, které v průběhu přípravy a realizace zadávacího řízení mohou nastat, a rizika s nimi spojená. Rozhodně se nejedná o vyčerpávající výčet způsobů zohlednění varování před kybernetickou hrozbou v zadávacím řízení.

V praxi se lze setkat se zadávacími řízeními, v rámci kterých jsou zadávací podmínky formulovány zejm. pomocí požadavků na výkon a funkci, přičemž konkrétní podoba technického provedení poptávaného plnění je v dispozici dodavatele (zadavateli např. nezáleží na tom, jakým konkrétním způsobem bude výsledku dosaženo). Zadavatel je tedy schopen provést analýzu rizik na jemu známá aktiva, nicméně některá (podpůrná) aktiva vyplynou až ze samotných nabídek (na tato tedy zadavatel není v době před zahájením zadávacího řízení objektivně schopen analýzu rizik provést).

Obecně lze konstatovat, že další postup zadavatele bude odvislý zejm. od charakteru předmětu veřejné zakázky a skutečnosti, zda jsou jím definované požadavky konečné, nebo zda o finální podobě dodávaného informačního nebo komunikačního systému plánuje s dodavatelem dále jednat.

6.1 Volba druhu zadávacího řízení a postup v něm

6.1.1 Otevřené a užší řízení

Tato podkapitola popisuje možný postup zadavatelů v případě, že se rozhodnou zadat veřejnou zakázku v otevřeném nebo užším řízení (obdobně je však třeba postupovat i ve zjednodušeném podlimitním řízení).

Tyto dva druhy zadávacího řízení jsou určeny především pro situace, kdy je zadavatel v zadávací dokumentaci schopen definovat veškeré jím požadované parametry poptávaného plnění. Zákon o zadávání veřejných zakázek výslovně stanoví, že zadavatelé nejsou v těchto druzích zadávacího řízení oprávněni s účastníky zadávacího řízení o podaných nabídkách jednat. Podané nabídky jsou tedy konečné (mohou být pouze objasněny či doplněny v souladu s § 46 ZZVZ) a jsou posuzovány a hodnoceny podle podmínek stanovených předem v zadávací dokumentaci. Tyto druhy zadávacího řízení kladou na zadavatele vysoké požadavky na specifikaci zadávacích podmínek, neboť ty musí být stanoveny předem v podrobnostech nezbytných pro účast dodavatele v zadávacím řízení. Zájemci o veřejnou zakázku totiž musejí být předem seznámeni s tím, jaké jsou požadavky zadavatele na podobu plnění a podle jakých kritérií a jakým způsobem budou jejich nabídky hodnoceny.

Neznalost všech technických aspektů poptávaného informačního nebo komunikačního systému přitom není překážkou pro využití otevřeného nebo užšího řízení v případě,

že zadavatel je srozuměn s tím, že konkrétní podoba technického provedení poptávaného systému je ponechána na dodavateli.

Otevřené a užší řízení naopak nejsou vhodnými typy zadávacích řízení pro případy, kdy je možné očekávat podání nabídky obsahující pro zadavatele určitým způsobem překvapivé řešení (které by s ohledem na své potřeby nemohl bez dalšího akceptovat), resp. kdy zadavatel předpokládá, že finální podoba dodaného plnění bude odvislá od dalšího jednání s dodavatelem.

Praktický postup

V případě, že zadavatel má stanoveny veškeré rozhodné parametry poptávaného systému předem (zbývající parametry nejsou pro zadavatele podstatné, nebo na trhu neexistuje více druhů řešení), je schopen na jemu známá aktiva provést hodnocení rizik. Výsledky hodnocení rizik pak budou determinovat podobu zadávacích podmínek. Současně musí mít zadavatel vyjasněno (tyto úvahy budou obsaženy zejm. v plánu zvládání rizik), zda v případě detekce neakceptovatelných rizik spojených s používáním prostředků dotčených společností (pokud tedy tato rizika nebudou i přes svou úroveň akceptována) postačuje pro jeho potřeby snížení rizik na akceptovatelnou úroveň za použití bezpečnostních opatření, která v danou chvíli přicházejí v úvahu, s vědomím toho, že hrozba nemusí být zcela eliminována, nebo zda je z hlediska ochrany dostupnosti, důvěrnosti a integrity dat obsažených v poptávaném systému nezbytné hrozbu zcela eliminovat, čehož zadavatel dosáhne pouze úplným zákazem použití prostředků dotčených společností.

Okamžik hodnocení rizik a výběru bezpečnostních opatření

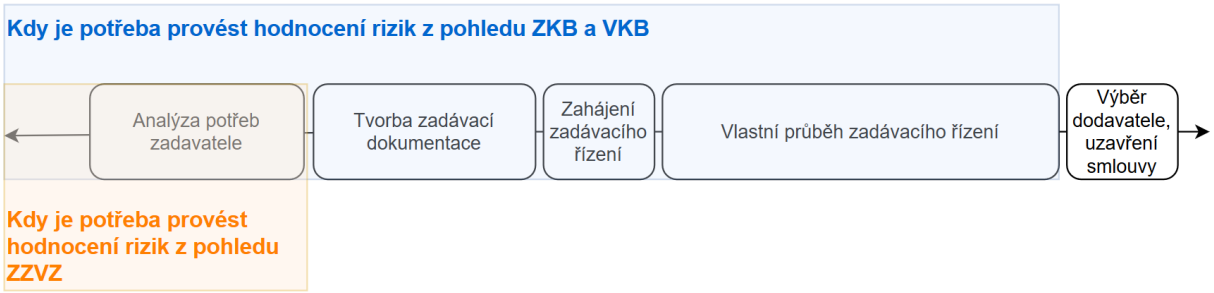
Ustanovení § 4 odst. 4 ZKB stanoví povinnost zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele, v případě zadavatelů zadávajících veřejnou zakázku v otevřeném nebo užším řízení tedy učinit požadavky vyplývající z bezpečnostních opatření součástí zadávacích podmínek. Analýza rizik je integrální součástí procesu hodnocení rizik, které je prováděno v rámci řízení rizik, tj. bezpečnostního opatření podle § 5 odst. 2 písm. b) ZKB. Dalším bezpečnostním opatřením, které je z podstatné části založeno na hodnocení rizik, je stanovení bezpečnostních požadavků pro dodavatele podle § 5 odst. 2 písm. e) ZKB, jehož součástí je řízení dodavatelů podle § 8 VKB. Podle § 8 odst. 2 písm. a) VKB jsou povinné osoby (tj. zadavatelé) u svých významných dodavatelů (tj. provozovatelů informačních nebo komunikačních systémů, resp. osob, se kterými vstupují povinné osoby do právních vztahů a které jsou významné z hlediska bezpečnosti informačních a komunikačních systémů) povinny provést v rámci výběrového řízení a před uzavřením smlouvy hodnocení rizik souvisejících s plněním předmětu výběrového řízení. Předpisy regulující kybernetickou bezpečnost tedy v určitých situacích zadavatelům nedávají na výběr, zda hodnocení rizik, jehož součástí je i analýza rizik, provedou před výběrem dodavatele nového systému, nebo až po implementaci nového systému do struktur zadavatele, naopak je výslovně stanoveno, že ve vztahu k významným dodavatelům se má

hodnocení rizik provést v rámci výběrového řízení, resp. před uzavřením smlouvy [srov. § 8 odst. 2 písm. a) VKB].

Zadavatel tedy splní své povinnosti vyplývající ze ZKB a VKB tím, že před uzavřením smlouvy s významným dodavatelem systému provede hodnocení rizik, tedy identifikaci, analýzu a vyhodnocení rizik, **a to v rozsahu informací, které jsou mu v době realizace zadávacího řízení známy**, a v návaznosti na výsledky procesu hodnocení rizik zanese požadavky na zajištění kybernetické bezpečnosti do smlouvy, kterou s vybraným dodavatelem uzavře.

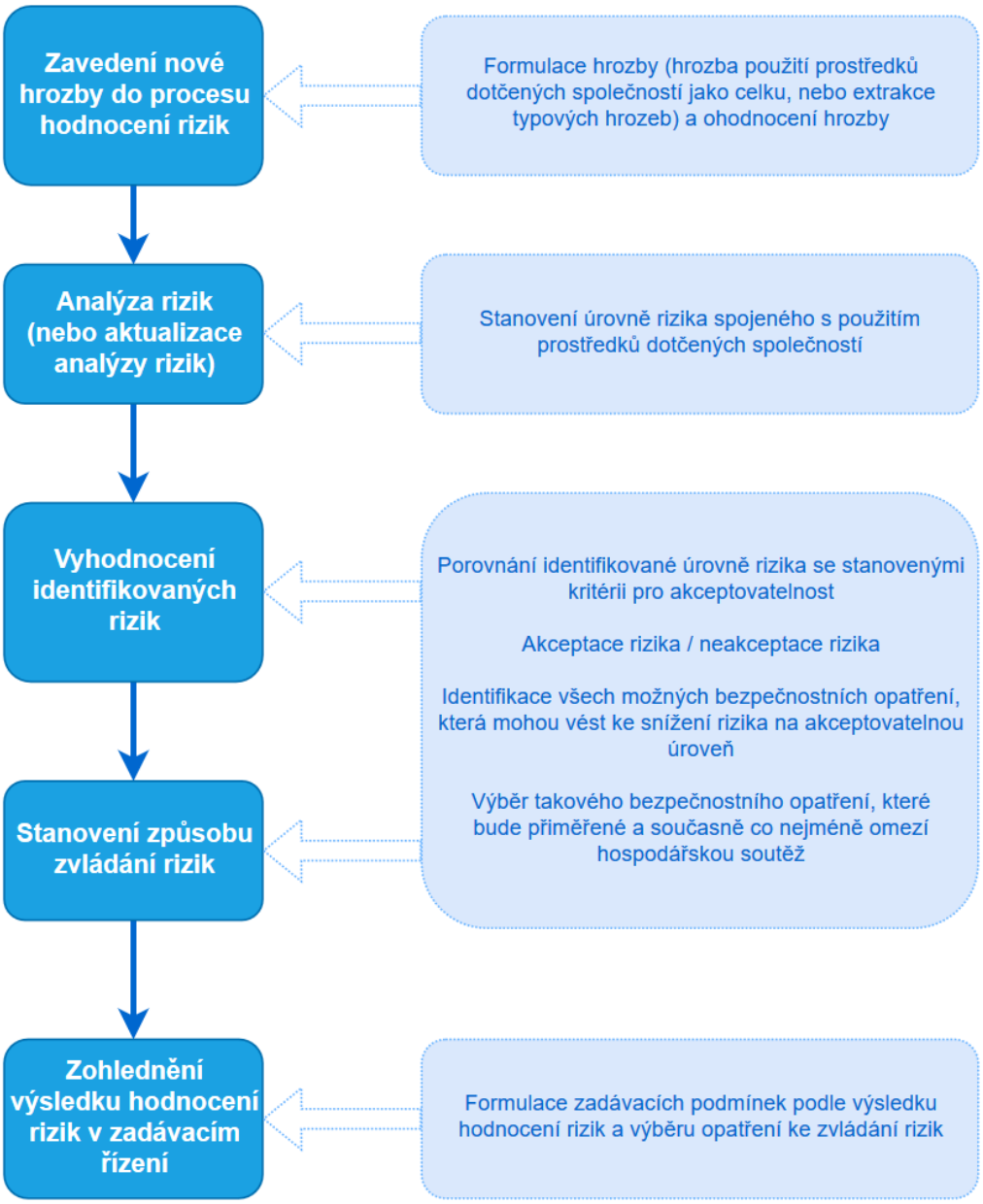
Pokud pak zadavatel volí pro zadání veřejné zakázky otevřené nebo užší řízení, u nichž je třeba stanovit všechny zadávací podmínky předem a o nabídkách již není možné dále jednat, musí být hodnocení rizik provedeno před samotným zahájením zadávacího řízení a požadavky na zajištění kybernetické bezpečnosti musí být součástí zadávacích dokumentace.

Výše popsaný postup shrnuje následující schéma:



Obrázek 2 Schéma určení okamžiku pro provedení hodnocení rizik v otevřeném nebo užším řízení

Postup zadavatele při stanovení zadávacích podmínek v tomto případě lze zjednodušeně znázornit následovně:



Obrázek 3: Schéma postupu zohlednění varování v otevřeném nebo užším řízení

Teoreticky pak lze uvažovat i o řešení spočívajícím v určitém zapojení dodavatelů do procesu hodnocení rizik (zadávací podmínky by musely krom požadavků na předmět plnění stanovit i způsob vypořádání se s požadavky ZKB a VKB, např. formou přenesení určitých činností na dodavatele nebo provedení určitých úkonů až ve fázi posuzování a hodnocení nabídek, včetně informací o tom, jakým způsobem mají dodavatelé při tvorbě svých nabídek postupovat a jak budou jejich nabídky následně posuzovány a hodnoceny). S ohledem na komplikovanost celého postupu a rizika s ním spojená (zejm. uveřejnění citlivých informací o systémech zadavatele, nezahrnutí všech podstatných informací do zadávací dokumentace a obdržení

nabídek, které nekorespondují s předpoklady zadavatele)[5] však doporučujeme držet se spíše výše popsaného postupu, příp. využít jednací řízení s uveřejněním, pokud zadavatel předpokládá, že o konkrétní podobě nabízeného plnění bude s dodavateli potřeba jednat (viz dále).

Současně je nezbytné upozornit, že pokud je poptáván systém, jehož finální technická podoba může zadavatele „překvapit" (tzn. může nastat situace, kdy je nabídnuto takové řešení, které zadavatel neočekával a které významně odporuje jeho předpokladům o nemožnosti přijetí „mírnějších" bezpečnostních opatření), není možné použití prostředků dotčených společností bez dalšího zakazovat.

Závěrem pak lze zmínit, že provedení hodnocení rizik před zahájením zadávacího řízení na základě informací, které zadavatel v tu chvíli má k dispozici, zadavatele nezbavuje povinnosti řídit aktiva a rizika s nimi spjatá i po výběru dodavatele a po implementaci dodaného systému do struktur zadavatele. Zadavatel tedy bude posléze povinen doplnit původně provedené hodnocení rizik o aktiva, příp. rizika, která mu před zahájením zadávacího řízení nebyla známa, a tato aktiva a rizika s nimi spjatá řídit v souladu s § 4 a § 5 VKB.

6.1.2 Jednací řízení s uveřejněním

Tato podkapitola popisuje možný postup zadavatelů v případě, že se rozhodnou veřejnou zakázku zadat v jednacím řízení s uveřejněním. Otevřené a užší řízení (příp. zjednodušené podlimitní řízení) totiž nejsou jedinými druhy zadávacího řízení, které mohou zadavatelé pro výběr dodavatele informačního nebo komunikačního systému využít.

Pokud např. není vhodné definovat předmět veřejné zakázky v dostatečných podrobnostech a zadavatel předpokládá, že o konkrétní podobě dodávaného plnění bude s dodavatelem dále jednat, může – za splnění zákonem stanovených podmínek – využít jednacího řízení s uveřejněním. Konkrétně lze uvažovat o využití § 60 odst. 1 písm. a) ZZVZ, dle kterého může zadavatel použít jednací řízení s uveřejněním v případě, že jeho potřeby nelze uspokojit bez úpravy na trhu dostupných plnění, nebo § 60 odst. 1 písm. b) ZZVZ, dle kterého může zadavatel použít jednací řízení s uveřejněním v případě, že součástí plnění veřejné zakázky je návrh

[5] Lze předpokládat, že zadavatel by musel uveřejnit mnoho citlivých informací o architektuře prostředí, do něhož bude dodávaný systém implementován, primárních i podpůrných aktivech, které jej tvoří, hodnotě, kterou pro něj jednotlivá aktiva (ať již jeho vlastní, či ta, která budou tvořit dodávaný systém) mají, dále by musel uveřejnit metodiku k hodnocení rizik, bezpečnostní politiky, plán zvládání rizik a další dokumenty, jejichž uveřejnění může pro zadavatele ve výsledku představovat bezpečnostní riziko. Nadto v případě, že zadavatel poptává systém, který dopodrobna nezná, jen stěží v zadávacích podmínkách pokryje všechny situace, ve kterých se může ocitnout (těžko lze např. vyhotovit návod na hodnocení aktiv, která v danou chvíli neznám). Dále si lze jen obtížně představit, jakým způsobem zadavatel předem zabezpečí, aby hodnocení rizik provedené dodavatelem nebylo tzv. podstřelené (tzn. aby rizika nebyla hodnocena mírněji, než jak by je hodnotil zadavatel; hodnocení aktiv a rizik bude vždy subjektivní a není možné jej stanovit ve 100 % podrobnostech předem), stejně jako si lze jen obtížně představit, jakým způsobem by zadavatel dodavatelům rozporoval jejich tvrzení, že určitá komponenta dodávaného plnění je z pohledu kybernetické bezpečnosti nedůležitá.

řešení nebo inovativní řešení.[6] Zákon přitom nestanoví míru „úpravy“ plnění nebo „dotváření“ řešení, tedy o jak rozsáhlé úpravy plnění nebo návrhy řešení se musí jednat, aby byly naplněny podmínky pro použití tohoto druhu zadávacího řízení. Nadto je v případě důvodu podle § 60 odst. 1 písm. b) ZZVZ rozlišován návrh řešení a inovativní řešení, v případě „pouhého“ návrhu by tedy neměla být vyžadována jeho inovativnost. Pokud tedy skutečně půjde o případ, kdy je potřeba dodávané plnění určitým způsobem upravit na míru požadavkům zadavatele, není důvod tento druh zadávacího řízení opomíjet.

Jednací řízení s uveřejněním naopak nebude možné využít tam, kde je poptáváno tzv. off-the-shelf řešení, tedy takový produkt, který může být okamžitě k dispozici a není třeba jej nijak upravovat podle specifických potřeb zadavatele [pouhou implementaci produktu do struktur zadavatele pravděpodobně nelze považovat za úpravu plnění nebo návrh řešení ve smyslu § 60 odst. 1 písm. a) a b) ZZVZ].

Výhodou jednacího řízení s uveřejněním je mj. skutečnost, že zadavatelé mohou v průběhu jednání měnit nebo doplňovat zadávací podmínky, zejména technické podmínky (za předpokladu, že nedojde ke změně minimálních technických podmínek a že o změně budou účastníci zadávacího řízení písemně informováni a bude jim poskytnuta lhůta k úpravě předběžných nabídek). Zadavatel je tedy oprávněn v průběhu zadávacího řízení měnit zadávací podmínky (s výjimkou minimálních technických podmínek) podle toho, jaká řešení mu jednotliví účastníci navrhnou, příp. jednat o obsahu nabídek podle toho, zda u některých účastníků vyvstane potřeba doplnění navrhovaného řešení např. o určitá bezpečnostní opatření. Změna zadávacích podmínek přitom může být založena mimo jiné i na výsledcích analýzy rizik, kterou zadavatel provede teprve po obdržení předběžných nabídek, nikoli již před zahájením jednacího řízení s uveřejněním (informace o tom, že v průběhu jednání bude provedena analýzy rizik a na jejím základě budou moci být měněny zadávací podmínky, zřejmě nemusí být obsažena v iniciačních zadávacích podmínkách, v praxi však uveřejnění takové informace již při zahájení zadávacího řízení doporučujeme).

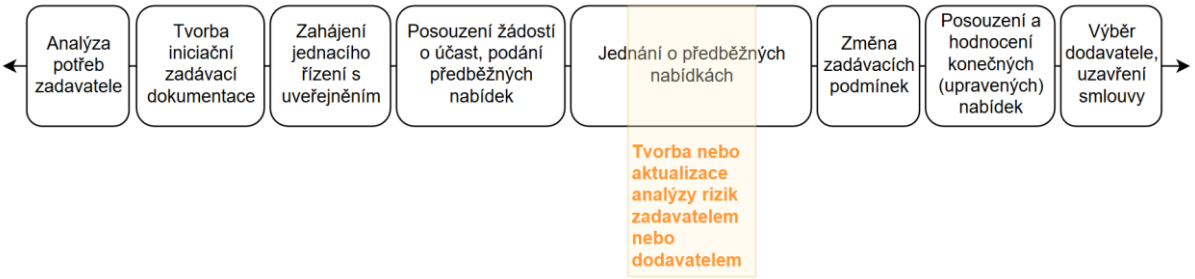
Zadavatelům je nadto dovoleno, aby si v zadávacích podmínkách vyhradili, že o podaných nabídkách nemusí být dále jednáno. Pokud tedy zadavateli vyhovuje již řešení navržené v předběžné nabídce, není nezbytné o obsahu nabídky dále jednat (tato možnost však musí

[6] Podle komentáře k ZZVZ autorů Dvořáka a kol. se bude zcela typicky jednat o případy, kdy součástí nabídek bude návrh řešení či projekt, který bude na základě navazujícího jednání mezi zadavatelem a účastníkem řízení dopracován dle individuálních potřeb zadavatele v jednotlivém případě. V rámci diskuze nad již konkrétním návrhem řešení v nabídce daného účastníka, které musí odpovídat minimálním technickým podmínkám vymezeným zadavatelem, má zadavatel dle autorů komentáře možnost s dodavatelem prodiskutovat své preference a představy ve vztahu k tomuto konkrétnímu návrhu řešení a v přímém dialogu s dodavatelem projednat možnosti úprav či dopracování tohoto řešení pro potřeby zadavatele. Naopak, cestou JŘSU by dle autorů komentáře neměly být řešeny takové veřejné zakázky, jejichž předmětem jsou produkty již v podstatě hotové či standardizované, běžné, které není nutné zásadním způsobem dotvářet či inovovat tak, aby vyhověly potřebám konkrétního zadavatele či okolnostem konkrétní veřejné zakázky. (Dvořák, D., Machurek, T., Novotný P., Šebesta, M. a kolektiv. *Zákon o zadávání veřejných zakázek. Komentář.* 1. vydání. Praha: Nakladatelství C. H. Beck, 2017, 1320 s.)

být explicitně vyhrazena v zadávací dokumentaci). I v takovém případě však zadavatel musí před výběrem dodavatele provést analýzu rizik.

V praxi by pak situace mohla vypadat tak, že zadavatel stanoví v zadávací dokumentaci požadavky na předmět plnění a označí, které z nich představují minimální technické podmínky, které musí nabídka splňovat. Zadávací podmínky budou nastaveny tak, že zadavatel na základě předběžných nabídek provede analýzu rizik a na základě jejích výsledků pak bude s účastníky zadávacího řízení jednat o případném doplnění bezpečnostních opatření nebo úpravě dodávaného plnění, aby bylo dosaženo uspokojivé úrovně kybernetické bezpečnosti. Výsledkem jednání může být dokonce i změna zadávacích podmínek v tom smyslu, že nebudou akceptována řešení, která obsahují prostředky dotčených společností, pokud je takové bezpečnostní opatření nezbytné.

Schematicky lze popsanou situaci vyjádřit následovně:



Obrázek 4: Schéma průběhu jednacího řízení s uveřejněním

Lze doplnit, že v případě podlimitních zakázek je zadavatelům umožněno využít jednací řízení s uveřejněním i bez splnění podmínek stanovených v § 60 ZZVZ.

7 Podřazení požadavku na vyloučení technických a programových prostředků dotčených společností ze zadávacího řízení pod konkrétní ustanovení ZZVZ

V případě zadávací podmínky definované jako zákaz použití prostředků dotčených společností v nabízeném řešení půjde o technickou podmínku ve smyslu § 37 odst. 1 písm. b) a § 89 ZZVZ, tedy o požadavek na vlastnosti předmětu veřejné zakázky, nikoli o požadavky na osobu dodavatele (zakázány jsou technické a programové prostředky určitého dodavatele, nejde o vyloučení samotného dodavatele, prakticky se zadávacího řízení může účastnit i dotčená společnost, nicméně nemůže nabídnout své vlastní výrobky). V případě, že dodavatel nabídne plnění, které i přes výslovný zákaz prostředky dotčených společností obsahuje, pak bude jeho nabídka ze zadávacího řízení vyřazena pro nesplnění zadávacích podmínek (§ 48 odst. 2 ZZVZ).

Fakticky dochází k vyloučení určité technologie, tedy k negativní definici technické stránky poptávaného plnění. Zákon o zadávání veřejných zakázek neumožňuje stanovit jiné zadávací podmínky (tj. podmínky kompletního průběhu procesu výběru dodavatele poptávaného plnění) než podmínky průběhu zadávacího řízení (zejm. lhůty, způsob komunikace, další parametry upravující praktický průběh zadávacího řízení), podmínky účasti v zadávacím řízení (kvalifikace dodavatelů, technické podmínky, obchodní nebo jiné smluvní podmínky a zvláštní podmínky plnění veřejné zakázky), pravidla pro snížení počtu účastníků zadávacího řízení nebo snížení počtu předběžných nabídek nebo řešení, pravidla pro hodnocení nabídek (tj. hodnotící kritéria) a další podmínky pro uzavření smlouvy na veřejnou zakázku (tj. předložení dokladů, vzorků, zabezpečení ochrany utajovaných informací nebo podmínky součinnosti před uzavřením smlouvy).

Půjde tedy o specifikaci poptávaného plnění, nikoli o požadavky na osobu dodavatele, ani o obchodní podmínky, kterými by se upravoval vztah smluvních stran v průběhu plnění veřejné zakázky, ani o hodnotící kritéria (zadavatel by sice mohl teoreticky hodnotící kritéria nastavit tak, aby nabídka obsahující prostředky vyloučených společností získala jen minimální počet bodů, nicméně zadavatel by tímto postupem riskoval, že taková nabídka bude muset být vybrána jako vítězná v případě, že se do zadávacího řízení nikdo jiný nepřihlásí, čímž by nebylo dostáno požadavkům ZKB).

8 Doporučená formulace zvoleného bezpečnostního opatření v otevřeném nebo užším řízení

Zadávací dokumentaci je nezbytné naformulovat tak, aby poskytovala dodavatelům všechny informace nezbytné pro jejich účast v zadávacím řízení, zejm. tedy pro vyhotovení a podání nabídek. Ze ZZVZ neplyne, že by součástí zadávacích podmínek mělo být též odůvodnění jednotlivých požadavků zadavatele. Není tedy nezbytné, aby zadávací dokumentace obsahovala veškeré podrobnosti o provedené analýze rizik a na ni navazujících dokumentech. Podrobnější informace může zadavatel poskytnout v rámci vypořádání námitek proti zadávacím podmínkám (odůvodnění rozhodnutí o námitkách musí obstát ve světle § 245 ZZVZ, musí se tedy podrobně a srozumitelně vyjadřovat ke všem stěžovatelem namítaným skutečnostem), resp. bude s vysokou pravděpodobností povinen je poskytnout v rámci případného správního řízení před ÚOHS (samotná analýza rizik sice nemusí být součástí dokumentace o zadávacím řízení, kterou je zadavatel ze zákona povinen ÚOHS zaslat, nicméně lze předpokládat, že ÚOHS si analýzu rizik a další související dokumenty může vyžádat v rámci kompletace podkladů rozhodnutí).

Doporučená struktura odůvodnění výběru technického/organizačního bezpečnostního opatření nebo zákazu použití prostředků dotčených společností v zadávacím řízení – nikoli nutně obsažená již v zadávací dokumentaci[7]:

1. Zadavatel je povinnou osobou podle ZKB.
2. Veřejná zakázka se týká informačního systému, u jehož správy a provozu je zadavatel povinen dodržovat ustanovení ZKB, tedy i zohlednit varování před kybernetickou hrozbou v procesu řízení rizik.
3. Zadavatel v reakci na vydání varování NÚKIB ze dne 17. prosince 2018 postupoval v souladu se ZKB a VKB, provedl analýzu rizik (resp. provedl aktualizaci stávající analýzy rizik – v závislosti na charakteru předmětu veřejné zakázky) a v návaznosti na výsledky analýzy zvážil všechna v úvahu přicházející bezpečnostní opatření ke snížení výsledné hodnoty rizika.
4. Na základě výsledků analýzy rizik a zvážení možností je třeba v případě nabídky technologie … dodat také … / doplnit řešení založené na rizikových technologiích o … / atd.

   NEBO

5. Jediným bezpečnostním opatřením, kterým je objektivně možné snížit hodnotu rizika na akceptovatelnou úroveň, je úplný zákaz použití prostředků dotčených společností v systémových strukturách zadavatele.

[7] Jde o strukturu, kterou doporučujeme v rámci možností konkrétního zadávacího řízení rozvést do větších podrobností (zejm. co se týče výsledků analýzy rizik a zvážení přijetí jiných bezpečnostních opatření).

Konkrétní text zadávací dokumentace je třeba přizpůsobit především tomu, co je předmětem veřejné zakázky a jak podrobné informace o charakteru poptávaného plnění zadavatel má, dále zda se veřejná zakázka týká nového či již existujícího informačního nebo komunikačního systému, zda je existující systém již určen systémem spadajícím pod ZKB, zda se nově vytvořený systém stane systémem spadajícím pod ZKB automaticky k okamžiku svého vzniku (např. naplněním odvětvových a dopadových kritérií významného informačního systému nebo naplněním definice systému určeného opatřením obecného povahy nebo rozhodnutím NÚKIB) nebo zda lze u nově vytvořeného systému předpokládat, že bude v dohledné době jako systém spadající pod ZKB určen.

Výše prezentovaná struktura úplného zákazu rizikových technologií v zadávacím řízení je dle názoru NÚKIB vhodná spíše pro plnění, u něhož zadavatel nedisponuje podrobnými informacemi o technickém provedení plnění, nemůže tedy zohlednit své dosavadní zkušenosti s řízením rizik u obdobných plnění a reaguje pouze na obecně definovanou hrozbu. Čím více informací o poptávaném plnění zadavatel má, tím podrobnější analýzu rizik je schopen provést a tím hlubší budou též jeho následné úvahy o přijetí jiných bezpečnostních opatření než úplného zákazu použití prostředků dotčených společností.

9 Rozhodovací praxe ÚOHS

Dne 6. listopadu 2019 vydal ÚOHS rozhodnutí **č. j. ÚOHS-S0262/2019/VZ-30266/2019/523/JMa**, kterým zamítl návrh společnosti Huawei Technologies (Czech) s.r.o. mířící proti zadávací podmínce spočívající v požadavku zadavatele (Ministerstva životního prostředí) na dodání druhého kusu hardware od nečínského výrobce ke každému kusu dodaného hardware od rizikového výrobce a jejich plnou společnou integraci tak, aby takové řešení plnilo funkci zajištění vysoké dostupnosti. Toto rozhodnutí nabylo právní moci dne 22. listopadu 2019 marným uplynutím lhůty pro podání rozkladu. Jde o první meritorní rozhodnutí ÚOHS ve věci zohlednění varování v zadávacím řízení.

V rámci správního řízení byl NÚKIB požádán o posouzení zadavatelem provedeného hodnocení rizik z hlediska požadavků ZKB a VKB a i na základě tohoto stanoviska ÚOHS konstatoval, že za dané situace zadavatel zvolil jediné možné řešení, kterým mohl dostát jak svým závazkům ze ZKB a VKB, tak povinnostem plynoucím ze ZZVZ.

Konkrétně ÚOHS mj. konstatoval, že *„Úřad (jakož ani NÚKIB) nevylučuje, že může – v teoretické rovině – existovat pro hospodářskou soutěž méně omezující technické opatření, než redundance, kterým by zadavatel zajistil vysokou dostupnost služby. Jak však Úřad uvádí v bodě 58. tohoto odůvodnění, zadavatel neměl (s ohledem na nedostupnost bližších informací) žádnou možnost takové opatření přijmout v situaci, kdy reálně nezná hrozbu, které čelí. Vedle úplného vyloučení řešení dotčených společností (které by bylo navíc „přísnějším" opatřením a bezpochyby by jej navrhovatel rovněž – stejně jako sporný požadavek – považoval za nepřiměřené) tak zadavatel sporným opatřením dle Úřadu v dané situaci zvolil pro něj jediné možné opatření pro zajištění vysoké dostupnosti služby. (…)*

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 rozhodnutí se ÚOHS dále vyjádřil k povinnosti zadavatele učinit analýzu rizik, potažmo další související informace, včetně odůvodnění výběru zvoleného bezpečnostního opatření pro mitigaci rizika, součástí zadávacích podmínek a v souladu s výše uvedeným konstatoval, že dokumenty obsahující analýzu (resp. celé hodnocení) rizik nejsou součástí zadávací dokumentace a informace o tom, na základě jakých podkladů zadavatel spornou podmínku stanovil, nejsou pro tvorbu nabídek do zadávacího řízení potřebné.

Celý text rozhodnutí je uveřejněn ve sbírce rozhodnutí ÚOHS dostupné zde: https://www.uohs.cz/cs/verejne-zakazky/sbirky-rozhodnuti.html.

Dne 13. ledna 2020 ÚOHS vydal další rozhodnutí týkající se postupu zadavatele při zohlednění varování v zadávacím řízení, **č. j. ÚOHS-S0358/2019/VZ-01269/2020/512/KMo**. Zadavatel, společnost Metropolnet, a.s., však v rozhodné době nebyl povinnou osobou podle § 3 ZKB,

z toho důvodu nebylo z jeho strany možné dovolávat se plnění povinností plynoucích ze ZKB a VKB. Text rozhodnutí je taktéž dostupný v internetové sbírce rozhodnutí ÚOHS.

Prozatím nejnovějším rozhodnutím ÚOHS, jež se dotýká varování NÚKIB, je rozhodnutí **č. j. ÚOHS-S0207/2021/VZ-27129/2021/500/AIv** ze dne 10. 8. 2021. Toto rozhodnutí nabylo právní moci dne 22. 10. 2021 vydáním rozhodnutí předsedy ÚOHS o rozkladu **č. j. ÚOHS-R0131/2021/VZ-32062/2021/163/MPe** ze dne 21. 10. 2021, kterým byl podaný rozklad zamítnut a napadené rozhodnutí potvrzeno.

Zadavatel (Česká správa sociálního zabezpečení) jakožto osoba povinná podle § 3 ZKB v zadávací dokumentaci stanovil zadávací podmínku, že za neakceptovatelné plnění je považováno takové plnění, které obsahuje technologie/klíčové prvky, vůči jejichž výrobcům vydal NÚKIB varování, a které současně bylo vyhodnoceno analýzou rizik jako plnění s vysokým až kritickým rizikem.

Nabídka dodavatele obsahovala technické a programové prostředky společnosti Huawei, tj. výrobce, vůči kterému vydal NÚKIB varování. Zadavateli přitom z provedené analýzy rizik vyplynulo, že dodavatelem nabízené technologické řešení představuje kritickou úroveň rizika. Na základě uvedeného se proto zadavatel rozhodl tohoto dodavatele vyloučit ze zadávacího řízení pro nesplnění uvedené zadávací podmínky.

Vyloučený dodavatel podal návrh k ÚOHS proti úkonu zadavatele spočívajícímu v rozhodnutí o jeho vyloučení s argumentační konstrukcí o nejasnosti zadávacích podmínek a jejich možném rozdílném výkladu. První stupeň i předseda ÚOHS se s těmito závěry navrhovatele neztotožnili, když v rozhodnutích uvedli, že ze znění zadávací dokumentace bylo zcela zřejmé, jaká technologická řešení nejsou akceptovatelná. Zákonnost stanovené zadávací podmínky přitom nebyla vůbec hodnocena, jelikož předmětem správního řízení byl přezkum postupu zadavatele spočívající ve vyloučení navrhovatele ze zadávacího řízení. Pokud chtěl navrhovatel zpochybnit zákonnost zadávacích podmínek, měl tak učinit vznesením námitek proti zadávacím podmínkám (a následným podáním návrhu), nikoli až námitkami proti svému vyloučení.

Předseda ÚOHS pak v rozhodnutí o rozkladu mj. konstatoval, že *„zadavatel, jakožto osoba povinná ke zpracování analýzy rizik, je v rámci této analýzy povinen zabývat se všemi hrozbami, které NÚKIB za hrozby označí, a zohlednit je. Volba konkrétního opatření je pak zcela v diskreci zadavatele.“*

Texty uvedených rozhodnutí jsou dostupné v internetové sbírce rozhodnutí ÚOHS viz odkaz výše.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
1. 3. 2020	1.0	Odb. regulace	Vytvoření dokumentu
7. 1. 2022	1.1	Odb. regulace	Doplnění rozhodovací praxe ÚOHS