MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX058P470
prvotní identifikátor

odbor provozu informačních technologií a komunikací
oddělení evidence obyvatel
Olšanská 4
Praha 3 130 27

Č. j. MV-150680-2/SIK5-2020

Praha 24. září 2020
Počet listů: 7

[redacted]

Rozhodnutí o odmítnutí Žádosti dle § 15 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Ministerstvo vnitra, odbor provozu informačních technologií a komunikací, (dále jen „**Ministerstvo vnitra**“ nebo „**povinný subjekt**“), jako povinný subjekt ve smyslu ustanovení § 2 odst. 1 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů (dále jen „**InfZ**“), obdrželo žádost o poskytnutí informací společnosti [redacted] (dále jen „**Žadatel**“), která je datována ke dni 9. 9. 2020 a doručena Ministerstvu vnitra dne 10. 9. 2020.

Z žádosti vyplývá, že Žadatel požaduje poskytnutí informací souvisejících s veřejnou zakázkou nazvanou „*Analýza proveditelnosti k využitelnosti pásma 400 MHz pro širokopásmové služby PPDR a k technickým a smluvním stránkám zřízení virtuálního operátora IZS*“, jejímž zadavatelem je Ministerstvo vnitra (dále jen „**Veřejná zakázka**“) a jejímž předmětem bylo zajištění dvou analýz (i) Analýza proveditelnosti k využitelnosti pásma 400 MHz pro širokopásmové služby PPDR (dále jen „**Analýza 1**“); a (ii) Analýza proveditelnosti technických a smluvních stránek zřízení virtuálního operátora IZS (dále jen „**Analýza 2**“). Zejména žádá Žadatel o následující informace:

„*poskytnutí veškerých výstupů souvisejících s Veřejnou zakázkou, zejména o poskytnutí Analýzy 1 a Analýzy 2 v kompletním znění, tedy vč. jakýchkoliv příloh, doplnění apod., vyhotovených společností Grant Thornton Advisory s.r.o., IČO 265 13 960, jako zhotovitelem.*“

Ministerstvo vnitra tuto žádost odmítá a

vydává

jako povinný subjekt dle ustanovení § 2 odst. 1 InfZ a v souladu s ustanovením § 15 a § 20 odst. 4 písm. a) InfZ, ve spojení s ustanovením § 67 a násl. zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů (dále jen „**správní řád**“) toto

ROZHODNUTÍ,

kterým se žádost o informace **odmítá v souladu s § 15 odst. 1 InfZ**.

Odůvodnění:

Žádost Žadatele se týká výstupů Veřejné zakázky, jejímž předmětem bylo vypracování Analýz 1 a 2 a dalších souvisejících dokumentů (zejména příloh zmíněných analýz, jejich doplnění apod.). Předmět těchto analýz úzce souvisí se způsobem zajištění komunikace bezpečnostních a záchranných složek – tedy systémem hromadné radiokomunikační sítě integrovaného záchranného systému (dále jen „**HRAS IZS**“). Tento systém HRAS IZS je prvkem kritické komunikační infrastruktury státu ve smyslu zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „**ZoKB**“) ve spojení s § 2 písm. g) zákona č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů (dále jen „**ZoKŘ**“). Prostřednictvím systému HRAS IZS je zajišťována veškerá komunikace integrovaných záchranných složek a ohrožení funkčnosti a integrity tohoto systému by proto mělo závažný dopad na bezpečnost státu, a to až s možnými dopady do ohrožení zájmů České republiky (zejména do ochrany majetku, života a zdraví osob).

Zvláštní skutečností se dle § 27 písm. 1 ZoKŘ rozumí „*údaje z oblasti krizového řízení, které by v případě zneužití mohly vést k znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života a zdraví osob, majetku, životního prostředí nebo podnikatelského zájmu právnické osoby nebo fyzické osoby vykonávající podnikatelskou nebo jinou obdobnou činnost podle zvláštních právních předpisů, pokud tyto údaje nejsou utajovanými informacemi*“.

Žádá-li osoba o poskytnutí informací, které jsou označeny za zvláštní skutečnosti ve smyslu § 27 ZoKŘ, řídí se poskytování těchto informací InfZ v souladu s § 2 odst. 3 InfZ, jelikož ZoKŘ neobsahuje komplexní úpravu procesu poskytování informací.

Dle § 27 odst. 8 ZoKŘ platí, že pokud „*právnická nebo fyzická osoba žádá orgán krizového řízení o informaci podle zvláštního právního předpisu, přičemž požadovaná informace je označena jako zvláštní skutečnost a žadatel k této informaci nemá oprávněný přístup, povinný subjekt žadateli tuto informaci neposkytne*“.

Povinný subjekt předně opakuje, že Žadatelem požadované informace se týkají systému HRAS IZS, jež slouží k zajištění komunikace složek integrovaného záchranného systému. Veškeré výstupy vzešlé z Veřejné zakázky, tedy zejména Analýzy 1 a 2, včetně všech jejich příloh, jež jsou požadovány v rámci žádosti Žadatele, jsou zvláštními skutečnostmi ve smyslu § 27 a násl. ZoKŘ a jako s takovými je nutné s těmito dokumenty také zacházet. Veškerá dokumentace vzešlá z Veřejné zakázky se dotýká oblasti krizového řízení subjektů účastnících se na provozu systému HRAS IZS a údaje uvedené v této dokumentaci (zejména v Analýzách 1 a 2), respektive jejich zveřejnění je způsobilé nežádoucím způsobem ohrozit zájmy České republiky, zejména ohrožení fungování systému HRAS IZS a s tím spojené omezení komunikace složek integrovaného záchranného systému (k tomuto blíže dále v textu).
Zvláštní skutečnosti musí být dle § 27 odst. 2 ZoKŘ formálně označeny jako takové skutečnosti, a to na svém nosném mediu – v uvedeném případě na listinách, které tvoří Analýzy 1 a 2, včetně všech doprovodných dokumentů. Veškeré výstupy Veřejné zakázky potom tuto skutečnost splňují a naplňují tedy formální znak zvláštních skutečností dle ZoKŘ.

Materiálně se potom zvláštní skutečnosti musí týkat informací, které mohou v případě jejich zneužití vést ke znemožnění či omezení činností týkajících se krizového řízení, respektive ohrožení života a zdraví osob nebo majetku. Jak již bylo zmíněno výše, požadované informace se týkají systému HRAS IZS a mohou obsahovat informace, které by v případě zveřejnění širokému okruhu osob bez jakéhokoliv omezení mohly zcela jistě vést k ohrožení funkčnosti tohoto systému a paralýze složek integrovaného záchranného systému (a s tím spojeným škodám na životu, zdraví a majetku obyvatel, respektive státu a státních institucí). Zveřejněním informací obsažených v Analýzách 1 a 2 může být ohroženo také zajišťování kybernetické bezpečnosti systému HRAS IZS. Nadto lze uvést, že zveřejněním těchto informací může dojít také k omezení či ohrožení systému krizového řízení, které je vykonáváno ze strany subjektů, které se účastní na provozu tohoto sytému HRAS IZS, jelikož jedním z aspektů úspěšného řešení krizových situací je právě omezení přístupu k některým informacím a detailům o daném systému kritické informační/komunikační infrastruktury, či budoucím fungování a technologiích týkajících se takového systému.

Žadatel v Žádosti neuvádí skutečnosti, které by dokládaly, že je osobou s oprávněným přístupem ke zvláštním skutečnostem ve smyslu § 27 ZoKŘ, přičemž

v případě žádosti o poskytnutí informací dle InfZ je možné tyto zvláštní skutečnosti poskytnout jen oprávněným osobám (§ 27 odst. 8 ZoKŘ). Vzhledem ke skutečnosti, že Žadatel neprokázal oprávněný zájem na zveřejnění jím požadovaných informací a zároveň není oprávněnou osobou k seznámení se se zvláštními skutečnostmi, je Ministerstvo vnitra nuceno jeho žádost odmítnout v souladu se zněním § 27 odst. 8 ZoKŘ. Povinný subjekt dále pro úplnost dodává, že Žadatel není účasten na systému krizového řízení systému HRAS IZS, ani není žádným jiným způsobem zapojen do správy či provozu této kritické infrastruktury a nesplňuje tedy žádné předpoklady, které by naplňovaly důvod pro seznámení se s požadovanými informacemi, které jsou zvláštními skutečnostmi.

Uvádí-li Žadatel v Žádosti, že jím požadované informace jsou pouze informacemi objektivními a statusovými a nevztahují se na ně žádné zákonné důvody, které by ospravedlňovaly jejich neposkytnutí, pomíjí přitom právě úpravu zvláštních skutečností dle § 28 ZoKŘ. Žadatelem požadované informace jsou zvláštními skutečnostmi, jejich zveřejnění je způsobilé znemožnit, omezit či ohrozit fungování kritické infrastruktury a činnosti subjektů, které se podílejí na její správě a provozu. Zveřejnění požadovaných informací by pak mohlo mít konkrétní dopady na činnosti týkající se krizového řízení, a to v podobě ohrožení bezpečnosti této infrastruktury spočívajícím v odhalení možných postupů a řešení nastalých situací a dále odhalit možné ochranné prvky kritické infrastruktury. V souvislosti s Analýzou 2 by případným zveřejněním požadovaných dokumentů mohly být široké veřejnosti (tedy také potenciálním útočníkům) poskytnuty informace o HRAS IZS, které obsahují detaily používaných technologií, jejich zabezpečovacích prvků a nastínit možná řešení a usnadnit tak provedení kybernetického či fyzického útoku na tento systém kritické infrastruktury státu. Analýzy obsahují také některé specifické údaje o současných technologiích HRAS IZS a zároveň o budoucích technologií, včetně návrhů možných řešení kritické infrastruktury, přičemž zveřejnění těchto údajů, a to i částečné, by mělo za následek vznik bezpečnostního rizika pro fungování systému HRAS IZS.

Ministerstvo vnitra pro úplnost v následující části tohoto rozhodnutí uvede konkrétní příklady dopadů zveřejnění Žadatelem požadovaných informací na ohrožení bezpečnosti systému HRAS IZS, zejména ohrožení krizových postupů v rámci procesu krizového řízení:

- Žadatelem požadované informace obsahují mimo jiné také údaje o operačních postupech jednotlivých subjektů v rámci krizového řízení, jejichž zveřejněním blíže neurčenému a nikým nekontrolovanému okruhu osob by mohlo dojít k ohrožení a narušení těchto operačních postupů v rámci jejich realizace – například v případě vzniku krizové situace by při znalosti těchto údajů útočníkem mohlo dojít k narušení těchto operačních postupů a znemožnění řádného výsledku vedoucímu k sanaci této krizové situace;

- Žadatelem požadované informace dále obsahují také detailní záměry Ministerstva vnitra v oblasti krizového řízení, a to vč. frekvenčního plánování či technických, organizačních a právních opatření k zajištění krizové komunikace, v případě zveřejnění takových informací by došlo ke značnému narušení účinnosti naplánovaných a stanovených procesů krizového řízení, jelikož v případně znalosti výše uvedených informací, lze tyto procesy předpokládat a snížit jejich dopady, případně je v určité části zcela znemožnit;
- Žadatelem požadované informace obsahují popis rizik stávajících postupů a zajištění krizové komunikace složek integrovaného záchranného systému (analýza rizik a přijímaných opatření), přičemž v případě znalosti těchto informací je možné snáze identifikovat citlivá místa systému HRAS IZS, což zvyšuje riziko úspěchu případného útoku na tento systém.

Lze tedy shrnout, že informace obsažené v Žadatelem specifikované dokumentaci, které se žádost týká, naplňují jak formální, tak materiální znaky zvláštní skutečnosti dle ZoKŘ, přičemž Žadatel není osobou s oprávněným přístupem k těmto informacím.
Shora popsaná nebezpečí, která souvisí se sdělením požadovaných informací, jsou dále ještě zvýšena povinností povinného subjektu podle § 5 odst. 3 InfZ do 15 dnů od případného poskytnutí informací zveřejnit tyto informace způsobem umožňujícím dálkový přístup, tj. na internetových stránkách povinného subjektu, čímž by se uvedené informace staly univerzálně a snadno dostupnými – tato situace je však s ohledem na právě popsaná rizika zcela nežádoucí.

Jak již bylo zmíněno výše, informace požadované v rámci žádosti Žadatele se týkají systému HRAS IZS, který je součástí kritické infrastruktury státu a jako takový tedy podléhá také povinnostem k zajištění kybernetické bezpečnosti dle ZoKB a na něj navazujících prováděcích předpisů. Z § 10a ZoKB potom výslovně vyplývá, že informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo jeho účinnost jsou vyloučeny z působnosti předpisů upravujících svobodný přístup k informacím (tedy také předpisu, dle kterého je podána žádost Žadatele).

Ačkoliv tedy Žadatel v žádosti uvádí, že „*obě Analýzy obsahují informace objektivní, statusové, a tedy nemají jiný než shrnující a analytický charakter*“, je na místě tuto žádost odmítnout, jelikož i zveřejněním údajně pouze shrnujících a analytických informací týkajících se využitelnosti pásem pro širokopásmové služby PPDR může dojít ke zveřejnění informací, které by v konečném důsledku mohly vést k ohrožení systému HRAS IZS, omezení či ztížení jeho provozu, omezení či úplné znemožnění postupů povinných subjektů v rámci krizového řízení a zajišťovaní kybernetické bezpečnosti, jak bylo ostatně Povinným subjektem shrnuto výše v tomto rozhodnutí.

Ministerstvo vnitra v této souvislosti odkazuje také na závěry uvedené v judikatuře, kterou bylo dovozeno, že i zveřejnění velmi obecných citlivých informací může

ohrozit bezpečnost chráněného objektu. Tyto závěry jsou uvedeny například v rozhodnutí Městského soudu v Praze, vedeného pod sp. zn. 10 A 42/2010, které je publikované ve sbírce rozhodnutí Nejvyššího správního soudu pod č. NSS 5685/2011. V tomto řízení Městský soud v Praze rozhodoval spor související s žádosti o poskytnutí informací týkajících se počtu a cen vozidel pořízených Policií ČR pro účely ochrany osob. Policie ČR odmítla žadateli tyto informace sdělit s odůvodněním, že by tyto informace mohly napomoci ke zjištění uplatňovaných opatření pro ochranu osob a s tím spojenému nepřiměřenému narušení bezpečnosti a Městský soud se k tomuto výkladu zcela přiklonil. Závěry uvedeného rozhodnutí je možné analogicky použít také v tomto řízení, kdy zpřístupnění i jen obecných informací o systému HRAS IZS, jakožto systému, prostřednictvím kterého je zajišťována komunikace integrovaných složek, který je navíc součástí kritické infrastruktury státu, je způsobilé ohrozit fungování těchto složek v důsledku ohrožení krizového řízení subjektů účastnících se na správě a provozu tohoto systému a dále také kybernetické bezpečnosti tohoto systému (zejména ohrožením krizového řízení, zjištěním informací o robustnosti tohoto systému, některých podrobností o jeho fungování či součástech, přičemž uveřejnění těchto informací široké veřejnosti je způsobilé narušit bezproblémovou funkčnost tohoto systému a tím paralyzovat činnost složek integrovaného záchranného systému).

V posuzované věci tedy také zveřejnění pouze obecných informací uvedených v Analýzách či dalších obecných údajů a informací vyplývajících z výstupů Veřejné zakázky může potenciálně ohrozit zájmy České republiky.

Poskytnutí předmětných informací by bylo rovněž v rozporu s prevenčními povinnostmi podle ZoKŘ, ZoKB a dalších relevantních právních předpisů souvisejících s povinnostmi Ministerstva vnitra v rámci správy a provozu systému HRAS IZS a v rámci činností týkajících se krizového řízení. Vzhledem k tomu, že poskytnutí informací a zejména jejich následné zveřejnění široké veřejnosti by mohlo vést mj. ke vzniku značných škod, je nutné zmínit rovněž obecné ustanovení § 2900 zákona č. 89/2012 Sb., občanského zákoníku, podle něhož platí, že vyžadují-li to okolnosti případu, je každý povinen počínat si při svém konání tak, aby nedošlo k nedůvodné újmě. V neposlední řadě lze alespoň obecně odkázat na celou řadu prevenčních povinností týkajících se zacházení se státním majetkem, jak jsou upraveny v příslušných právních předpisech. Povinný subjekt tedy závěrem uvádí, že explicitní důvody pro odmítnutí, které jsou zmíněny výše, jsou ještě posíleny těmito prevenčními povinnostmi.

Na základě uvedeného proto bylo rozhodnuto tak, jak je uvedeno ve výroku tohoto rozhodnutí.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Poučení:
Proti rozhodnutí máte právo podat v souladu s ustanovením § 16 InfZ a § 152 správního řádu rozklad, a to ve lhůtě 15 dnů ode dne doručení této odpovědi. Rozklad se podává k Ministerstvu vnitra, nejlépe cestou odboru provozu informačních technologií a komunikací, o rozkladu rozhoduje ve smyslu § 152 odst. 2 správního řádu ministr vnitra.

Mgr. Bohdan Urban
ředitel