Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

DŮVODOVÁ ZPRÁVA

Vyhláška o kritériích rizikovosti dodavatele

A. Obecná část

a) Vysvětlení nezbytnosti navrhované právní úpravy, odůvodnění jejích hlavních principů

V návrhu zákona o kybernetické bezpečnosti (dále také „Zákon“), transponujícího zejména směrnici Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (dále jen „směrnice NIS2“), rovněž dochází k právní úpravě mechanismu prověřování bezpečnosti dodavatelského řetězce (dále jen „Mechanismus posuzování dodavatelů“). Tento institut usiluje o vytvoření komplexního a transparentního procesu prověřování dodavatelů do kritických částí stanoveného rozsahu podle § X odst. 1 *[Prověřování rizik spojených s dodavatelem]* zákona. V § X odst. 1 *[Omezení rizik spojených s dodavatelem]* je stanoven specifický způsob, jakým lze reagovat na rizikovost konkrétního dodavatele bezpečnostně významné dodávky, a sice vydáním opatření obecné povahy, na základě kterého může dojít k omezení či dokonce zakázání využití jeho plnění.

Jedním z cílů navrhované zákonné úpravy je přispět k zajištění dlouhodobě udržitelné bezpečnosti České republiky (dále také „ČR“) prostřednictvím zabezpečení a zvýšení odolnosti osob a institucí, jež jsou nezbytné pro naplňování základních funkcí státu, s minimalizací zásahu do vlastnických práv podnikatelů.

V posledních letech posiluje trend klást důraz na kybernetické zabezpečení informačních technologií, zvláště těch, které zajišťují základní funkce společnosti, a vznikají nové standardy a právní regulace, jež motivují osoby a orgány veřejné moci k zavádění kybernetických bezpečnostních opatření. Je nicméně zřejmé, že úroveň kybernetické bezpečnosti produktů a služeb informačních a komunikačních technologií (dále jen „ICT“) je závislá nejen na zavedení bezpečnostních opatřeních a jejich technickém provedení, ale i na dodavatelích ICT produktů či služeb.

Dodavatelé mají v ICT infrastruktuře výsadní postavení. Hardwarová a softwarová řešení ICT jsou již natolik komplexní a v infrastrukturách povinných osobo mechanismu tak četně zastoupená, že je nelze technicky komplexně včas a efektivně prověřovat.

I s ohledem na časté aktualizace je technické testování ICT produktů ve velkém měřítku vysoce neefektivní. Problematika bezpečnostních záplat taktéž ztěžuje správcům infrastruktury technicky ověřit implementovaná softwarová řešení od svých dodavatelů, jelikož v případě odhalení (i zcela neúmyslných) slabin je potřeba co nejrychleji vydat softwarové aktualizace, než jich využijí útočníci (tzv. zranitelnosti nultého dne[1]). Takové aktualizace proto nemohou být podrobeny důkladné analýze, a nelze tak vyloučit riziko, že budou obsahovat například zadní vrátka, nebo jiný škodlivý kód. Klíčovým faktorem zabezpečení ICT je proto důvěra

[1] Dle Zprávy o stavu kybernetické bezpečnosti za rok 2021 se jedná o typ zranitelnosti, který bývá často využíván např. cizím státem podporovanými skupinami.

v dodavatele, že nezneužije své výsadní postavení ve prospěch svůj, státu, který má na dodavatele vliv, či jiného aktéra.

Dodavatele ze zemí majících např. nestandardní legislativní prostředí umožňující ingerenci státních aktérů do produktů, služeb či procesů dodavatelů, a jejichž zájmy jsou v konfliktu se zájmy ČR a jejích spojenců, lze považovat za rizikové. Ačkoliv výrobci či dodavatelé ICT produktů a služeb (dále jen „dodavatelé ICT“) mají s ohledem na generování zisku zájem o prodej kvalitních a bezpečných produktů, ne vždy se musí jednat o jejich jediný zájem.

Dodavatelé ICT mají sídla v různých zemích a podléhají rozličným právním řádům, mocenským strukturám a jiným neobchodním vlivům. Zvýšené riziko představují primárně dodavatelé ICT z autoritářských států, které mají silný vliv na své domácí společnosti a neváhají jej využít pro prosazování svých geopolitických cílů, jež mohou být v rozporu se zájmy ČR či jejích spojenců. Dodavatel ICT může být natolik propojený a ovlivněný státním a politickým aparátem své domovské země, že bude nezřídka činit i ekonomicky kontraproduktivní rozhodnutí v souladu se zájmy režimu, který mu potenciální reputační škodu může kompenzovat, popřípadě jej za jednání v rozporu se svými zájmy potrestat. Navíc, vzhledem k obtížnému odhalení, a ještě obtížnější atribuci (přičitatelnosti) kybernetických útoků[2], mohou tyto aktivity představovat pro výrobce přijatelné riziko, které mu zajistí výhodné postavení v domovském státě a výrazněji neohrozí jeho zisk.

V řadě států mohou být společnosti také nuceny ke spolupráci se zpravodajskými službami státu prostřednictvím právních předpisů, které je ke spolupráci zavazují. V Čínské lidové republice (dále také „ČLR“) ukládá legislativa povinnost jednotlivcům i společnostem spolupracovat s čínskými státními autoritami. Jedná se např. o mechanismus, který je začleněný v zákoně o společnostech z roku 2013, jež ukládá všem společnostem povinnost ustanovit uvnitř svých struktur stranickou organizaci Komunistické strany ČLR (dále jen „KS ČLR“), pokud ve společnosti pracují nejméně tři členové strany. V praxi to znamená přímý dosah této strany na dění v jakékoliv významné společnosti. KS ČLR vykonává skrze stranické organizace přímou kontrolu nad společnostmi a zajišťuje, že beze zbytku plní, co se od nich očekává, včetně požadavků v oblasti státní bezpečnosti.[3] Čínský zákon o kybernetické bezpečnosti z roku 2017 pak obsahuje řadu ustanovení stanovujících povinnost spolupráce se státními orgány. Článek 28 zákona o kybernetické bezpečnosti určuje povinnost provozovatelů sítí poskytnout technickou podporu a spolupráci orgánům veřejné bezpečnosti a orgánům státní bezpečnosti.[4] Zákon o státní zpravodajské činnosti z téhož roku zdůrazňuje, že relevantní státní instituce jsou oprávněny vyžadovat spolupráci po jednotlivcích a organizacích: „*Národní zpravodajské služby mohou v souladu se souvisejícími státními předpisy požádat příslušné orgány, organizace a občany o poskytnutí potřebné podpory, součinnosti a spolupráce*.“.[5]

[2] Atribuce dle vyjádření NÚKIB představuje proces, během něhož dochází k určení pravého zdroje útoku a samotného útočníka. Dostupné zde: https://www.nukib.cz/cs/infoservis/aktuality/1735-bezpecnejsi-zdravotnictvi-i-reseni-rizikovych-dodavatelu-vlada-schvalila-akcni-plan-ke-strategii-kyberneticke-bezpecnosti/

[3] Law Bridge. 28.12.2013. Dostupné zde: http://www.lawbridge.org/zhong-hua-ren-min-gong-he-guo-gong-si-fa-2013-nian-xiu-ding/

[4] Cyberspace Administration of China. 2017. 中华人民共和国网络安全法. Dostupné zde: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm

[5] National People’s Congress of the People’s Republic of China. 2017. 中华人民共和国国家情报法. Dostupné zde: http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

Taktéž Ruská federace (dále jen „RF“) přijala během poslední dekády několik zákonů s významným dopadem v oblasti kybernetické a informační bezpečnosti, které zásadním způsobem zasahují do fungování soukromých společností.[6] Zákon o Federální službě bezpečnosti (FSB) RF (40-FZ) poskytuje státu právní nástroje donucení ke spolupráci formálně soukromé entity, a to včetně globálně působících výrobců ICT.[7] Ustanovení § 15 tohoto zákona umožňuje FSB instalovat dodatečný software a hardware do ICT produktů ruských společností[8], stejně tak jako dosazovat do jejich struktury důstojníky FSB.[9] Jedním z konkrétních případů osazeného softwaru je systém SORM (Systém pro operativní vyšetřovací činnost). Ten umožňuje FSB a dalším ruských bezpečnostním složkám monitoring síťového provozu zejména na ruském území. Slouží tak k získávání informací, sledování osob či digitální cenzuře a je primárně nasazen na síťovém provozu v rámci Ruské federace. V rámci ukrajinského konfliktu však Rusko přistoupilo k přesměrování síťového provozu na okupovaných územích právě skrze ruské poskytovatele a infrastrukturu, což ruským bezpečnostním složkám umožnilo systém SORM používat pro výše zmíněné účely i na území Ukrajiny. Okupační autority tak získaly informační kontrolu i nad tamním okupovaným obyvatelstvem.

Také Írán velmi pravděpodobně disponuje kapacitami narušit dodavatelský řetězec, nicméně limitují ho dva výrazné faktory. Těmi jsou technologická zaostalost ve srovnání s Ruskem nebo Čínou a omezení záběru útoků hlavně na Blízký východ (primárně Izrael a Saúdská Arábie) či USA. V případě technologické zaostalosti je třeba brát v potaz, že v islámské republice neleží významné výrobní kapacity hardwaru (na rozdíl od ČLR) ani softwaru (na rozdíl od ČLR a RF), což Teheránem zaštítěným aktérům ztěžuje možnost kompromitace. Přesto země disponuje ofenzivními schopnostmi a technicky vzdělanou populací, kterou ekonomické sankce a nemožnost uplatnit se na legálním trhu práce často nutí participovat na škodlivých aktivitách. Právně-regulační mechanismy srovnatelné s Ruskem a Čínou nejsou v Íránu veřejně známé, nicméně existují důkazy o tom, že mnoho domácích softwarových produktů je kompromitováno za účelem sledování opozice a potlačování disentu. Nelze tedy vyloučit, že Írán přijal vlastní restriktivní zákony v této oblasti.

Přestože i v ČR, stejně tak jako v dalších zemích Evropské unie a spojeneckých zemích ČR, existuje legislativa regulující vztah státu a soukromých společností pro potřeby zajišťování obrany státu a národní bezpečnosti[10], pravomoci státu jsou ve srovnání s těmi čínskými či ruskými nepoměrně nižší, případné zásahy musejí být řádně odůvodněné, podléhají soudnímu přezkumu a usilují o co nejmenší rozsah získávaných informací.

Dodavateli (či s jejich asistencí) způsobené úmyslné narušení kybernetické bezpečnosti strategicky významné infrastruktury, a to zejména nejzávažnější případy, jako je narušení dostupnosti systému ve velkém rozsahu, představuje podstatný problém pro významné

[6] Human Rights Watch. 2020. Russia: Growing Internet Isolation, Control, Censorship. Dostupné zde: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship

[7] Peter B. Maggs. 2018. Report of Peter B. Maggs. Dostupné zde: https://assets.documentcloud.org/documents/4386053/Report-of-Peter-B-Maggs-Russian-Surveillance-Law.pdf

[8] Федеральный закон от 03.04.1995 N 40-ФЗ (ред. от 02.12.2019) "О федеральной службе безопасности" (Federal Law on the Federal Security Service of the Russian Federation); Venice Commission. 2012. Federal Law on the Federal Security Service of the Russian Federation.

[9] FSB Dossier. 2020. Аппарат прикомандированных сотрудников. Dostupné zde: https://fsb.dossier.center/prikom/

[10] V České republice se jedná zejména o Zákon č. 289/2005 Sb., o Vojenském zpravodajství.

ekonomické zájmy a bezpečnost státu, jelikož mohou výrazně narušit fungování státu, ekonomiky, společnosti a v krajním případě ohrozit zdraví a životy obyvatel.

Přestože jsou popsaná rizika spojená s dodavateli známá, v současnosti neexistuje v ČR komplexní mechanismus, který by umožnil rizika plynoucí z těchto strategických hrozeb pro strategicky významnou infrastrukturu cíleně, účinně a flexibilně vyhodnocovat a mitigovat.

Legislativní požadavky na národní i unijní úrovni v technické rovině zajišťování kybernetické bezpečnosti vedou ke zvyšování zabezpečení ICT na národní úrovni, a to především v infrastruktuře regulované zákonem o kybernetické bezpečnosti, mezi kterou je i strategicky významná infrastruktura. Útočníci tak musejí vynakládat stále vyšší úsilí směřující k narušení a nepozorovanému působení ve strategicky významných informačních systémech, což je zpravidla hlavní cíl škodlivého aktéra, jehož cílem je dlouhodobě narušovat důvěrnost, integritu či dostupnost informací přenášených těmito systémy. Takoví útočníci se musejí adaptovat na nové prostředí a vyhledávat nové vektory útoků. I to je jedním z důvodů zvyšující se atraktivity provádění útoků na dodavatelský řetězec, popř. využívání dodavatelů k prosazování cílů těchto škodlivých aktérů.

Jednou z primárních funkcí státu je zajištění vnitřní bezpečnosti a vnější obrany. Stát je garantem zachování bezpečnosti občanů, jejich majetku, veřejného pořádku a státních zájmů a územní celistvosti a nedotknutelnosti. Na tyto funkce by neměl rezignovat tím, že je přenese na třetí, často soukromé, osoby. Stát proto nemůže ponechat výhradní výběr potenciálně rizikového dodavatele strategicky významné infrastruktury zcela v rukou soukromých společností, které nemusí být dostatečně vybaveny nebo motivovány k ochraně bezpečnosti ČR. Ačkoliv mají soukromé společnosti zájem o poskytování kvalitních a bezpečných produktů a služeb, jejich primárním cílem je dosažení zisku, přičemž tyto dva aspekty (bezpečnost versus dosažení zisku prostřednictvím minimalizace nákladů) mohou být v určitých případech v přímém rozporu a mohou upřednostnit vyšší zisk na úkor bezpečnosti. V souladu s čl. 1 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění pozdějších předpisů, podle kterého je základní povinností státu: „*zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových hodnot*“ musí stát ze své podstaty na takové riziko reagovat a usilovat o jeho mitigaci.

V zájmu státu je proto prověřovat strategickou rizikovost dodavatelů, kteří mohou poskytovat plnění v rozsahu bezpečnostně významných dodávek[11], a to jak na základě posouzení kritérií souvisejících se samotným dodavatelem, tak na základě posouzení státu, který na něj má vliv.

Samotné prověřování strategické rizikovosti dodavatele přitom nelze ponechat na dotčených poskytovatelích regulované služby, neboť tito z povahy věci nemohou disponovat dostatečnými informacemi nutnými ke kvalifikovanému posouzení. Oproti tomu stát má kapacity a orgány, díky kterým může tyto informace zjišťovat, a je proto lépe vybaven k prověření strategické rizikovosti dodavatele. Nicméně není možné nechat na svévoli státu, jak bude při prověřování rizikovosti postupovat, což by mohlo vést k neodůvodněným

[11] Plnění, které směřuje do kritické části stanoveného rozsahu dle § X odst. 1 *[Prověřování rizik spojených s dodavatelem]* zákona.

a netransparentním omezením dodavatelů a popření principu právního státu, kdy státní moc může být vykonávána pouze na základě zákona.

Nutno podotknout, že dle výsledků dotazníkového šetření[12], i správci strategicky významné infrastruktury vyhodnocují některá kritéria související s netechnickými aspekty dodavatelů či nabízených technických řešení. Jedná se zejména o posuzování a vyhodnocování kritérií souvisejících se sídlem dodavatele (zdali má dodavatel sídlo v zemi EU či NATO vyhodnocuje 72 % respondentů, zdali dodavatel podléhá právním řádům zemí, na které veřejně upozorňují bezpečnostní instituce ČR vyhodnocuje 66 % respondentů. Vlastnickou strukturu dodavatele zná a vyhodnocuje 69 % respondentů. Zdali byl dodavatel pravomocně odsouzen pro trestný čin zajímá 55 % respondentů, o poznání méně respondentů (32 %) pak hodnotí, zdali je dodavatel pod výkonem účinné míry kontroly hospodářské činnosti cizího státu, resp. zdali dodavatel jedná eticky, v souladu s pravidly mezinárodního obchodu a s péčí řádného hospodáře (35 %). Další hrozby spojené s dodavatelským řetězcem jako hrozba nedodržení smluvního závazku ze strany dodavatele nevyhodnocuje 11 % respondentů, hrozbu zneužití vnitřních prostředků či sabotáž nevyhodnocuje 20 % respondentů a hrozbu použití špionážních technik ze strany či prostřednictvím dodavatele nevyhodnocuje dokonce 38 % respondentů.

Bez navrhované právní úpravy by posuzování a vyhodnocování takovýchto kritérií či hrozeb i nadále zůstalo zcela na vůli a míře posouzení samotných správců strategicky významné infrastruktury a nebylo by vyžadováno, aby k posuzování takového typu kritérií docházelo. Absence posuzování strategických rizik plynoucích ze strany dodavatelů do významné strategické infrastruktury by tak nebyla výjimečná, a jelikož značná část dotázaných subjektů takovou analýzu neprovádí nyní, existuje velice nízká pravděpodobnost, že by došlo ke změně jejich přístupu k této problematice bez regulatorních nástrojů. V krajních případech by tak mohlo dojít k narušení až ochromení fungování některé strategicky významné infrastruktury, což by mělo celospolečenský dopad.

Z toho důvodu Zákon zavádí kritéria rizikovosti dodavatele (dále také jako „kritéria“), přičemž až po vyhodnocení jejich naplnění je možné omezit plnění povinným osobám mechanismu v rozsahu poskytování bezpečnostně relevantních dodávek identifikovaného rizikového dodavatele. Účelem zavedení kritérií je zajištění transparentnosti všech obecných hledisek, které mají význam pro posouzení, zda konkrétní dodavatel představuje hrozbu pro bezpečnost ČR nebo vnitřní či veřejný pořádek. Důraz je tak kladen na význam hrozby plynoucí ze strany bezpečnostně rizikového dodavatele nejen pro povinné osoby mechanismu, ale i pro bezpečnost státu jako takového. Existence kritérií navíc posiluje právní jistotu samotných dodavatelů a poskytovatelů regulované služby povinných z mechanismu posuzování dodavatelů, neboť jednoznačně stanovují, jaké skutečnosti stát považuje za významné pro posouzení rizikovosti dodavatele. V důsledku proto dojde k eliminaci úřední svévole a k vytvoření spravedlivého a transparentního procesu, jelikož k omezení dodavatele (ať už formou varování nebo opatření obecné povahy) může dojít jen při naplnění konkrétně stanovených kritérií.

[12] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, kteří se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

Zákon samotný kritéria neobsahuje a předpokládá jejich stanovení v prováděcím právním předpise – vyhlášce, k jehož vydání zmocňuje Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“).

Tento návrh vyhlášky předkládá NÚKIB na základě zmocnění uvedeného v § X zákona o kybernetické bezpečnosti, k provedení obsahu § X tohoto zákona.

b) Zhodnocení souladu návrhu vyhlášky s ústavním pořádkem České republiky a se zákonem, k jehož provedení se navrhuje

Návrh vyhlášky je v souladu s ústavním pořádkem České republiky.

Důvodová zpráva k Zákonu se vypořádává s faktem, že oblast kybernetické bezpečnosti se z hlediska právních předpisů, které jsou součástí ústavního pořádku, dotýká především práva vlastnického a částečně též i z něj odvozovaného práva na svobodu podnikání dle Listiny základních práv a svobod. Povinnosti, které navrhovaná zákonná právní úprava stanoví vybraným subjektům (tzv. poskytovatelům regulované služby), totiž v různé míře omezují tyto subjekty v užívání systémů, k nimž vykonávají vlastnická nebo obdobná práva.

Úzce vymezené části poskytovatelů regulované služby s potenciálně největšími dopady pro fungování České republiky může zákon o kybernetické bezpečnosti omezit vlastnické právo, resp. právo na podnikání, v rámci nově zaváděného mechanismu posuzování dodavatelů. V případě, že dodavatel bude shledán rizikovým a dojde k vydání opatření obecné povahy (dále jen „OOP“), je poskytovatel regulované služby, kterému plynou povinnosti z mechanismu posuzování dodavatelů, povinen vyloučit dodavatele ze svých kritických částí stanoveného rozsahu dle podmínek stanovených ve vydaném OOP. Pokud bude vydáno varování, poskytovatel regulované služby, kterému plynou povinnosti z mechanismu posuzován dodavatelů, je povinen varování zohlednit při hodnocení rizik a v plánu zvládání rizik, což může vyústit rovněž ve vyloučení dodavatele z bezpečnostně relevantních dodávek do kritické části stanoveného rozsahu. V obou případech proto dochází k relativně citelnému zásahu do práva na vlastnictví, resp. práva na podnikání.

Byť vydání varování a OOP svým charakterem vytváří povinnosti jen pro dotčené poskytovatele regulované služby, fakticky má velmi citelný dopad i na samotné dodavatele, kteří mohou být nepřímo vyloučeni z dodávání plnění pro konkrétní množiny poskytovatelů regulovaných služeb. Zákon, a v důsledku i navrhovaná vyhláška, proto zasahuje i do práva na podnikání dodavatelů, kteří budou shledáni rizikovými a bude proti nim vydáno varování či opatření obecné povahy.

Zákon, který navrhovaná vyhláška provádí, se vypořádal s odůvodněním narušení výše uvedených práv následovně.

Možné omezení práva na užívání majetku, za které by snad povinná bezpečnostní opatření uložená tímto Zákonem a jeho budoucími prováděcími předpisy mohla být považována, má za účel chrání obecné zájmy, kterými je bezpečnost státu a obyvatelstva či významné ekonomické a společenské zájmy. Kybernetická bezpečnost České republiky jako podmnožina bezpečnosti České republiky spadá do rozsahu působnosti ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. Podle čl. 1 uvedeného ústavního zákona je zajištění svrchovanosti a územní celistvosti České republiky, ochrana jejích demokratických základů a ochrana životů, zdraví a majetkových

hodnot základní povinností státu. Zákon lze považovat za jeden z prostředků plnění této povinnosti státu. Zákon zároveň reflektuje postavení kybernetické bezpečnosti jako nedílného předpokladu rozvoje digitální společnosti a ekonomiky, o nějž ČR jako členský stát Evropské unie usiluje.

Navrhovaná vyhláška je zcela v souladu se shora uvedeným, neboť důsledně sleduje smysl a účel Zákona a v jeho rámci Mechanismus posuzování dodavatelů. Návrh vyhlášky na základě Zákona a v jeho mezích stanovuje kritéria rizikovosti dodavatele, tak aby byla zcela transparentní obecná hlediska, která mohou vést k vydání varování nebo OOP. Akcent je přitom kladen na přiměřenost a nezbytnost kritérií, tak aby zásah do ústavou zaručených práv a svobod byl minimalizován. Navrhovatel zvolil cestu redukce kritérií pouze na ta, která zcela jednoznačně mohou zavdat pochybnost o bezpečnostní rizikovosti či důvěryhodnosti dodavatele, resp. která mohou zvyšovat riziko, že prostřednictvím dodavatele dojde ke kybernetickému bezpečnostnímu incidentu. Současně obsahem navrhované vyhlášky je pouze stanovení kritérií, což je plně v souladu se zmocňovacím ustanovením v Zákoně.

c) Zhodnocení souladu návrhu vyhlášky s mezinárodními smlouvami, jimiž je Česká republika vázána, judikaturou ESLP a s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

V oblasti kybernetické bezpečnosti nebyla dosud uzavřena žádná mezinárodní smlouva. Druhotně se kybernetické bezpečnosti dotýká Úmluva Rady Evropy o kyberkriminalitě, rovněž známá jako Budapešťská úmluva. Zákon o kybernetické bezpečnosti a jeho prováděcí předpisy včetně tohoto návrhu vyhlášky jdou rovněž v duchu nezávazných doporučení a závazků chránit důležité informační systémy formulovaných například ve zprávách Skupiny expertů OSN (UN GGE) či v opatřeních pro budování důvěry přijatých účastnickými státy Organizace pro bezpečnost a spolupráci v Evropě.

Přímo se kybernetické bezpečnosti nedotýká ani judikatura Evropského soudu pro lidská práva. Problematiku související s návrhem právního předpisu lze posuzovat z hlediska práv chráněných Evropskou úmluvou o lidských právech, např. práva na pokojné užívání majetku (povinné zavádění bezpečnostních opatření), práva na respektování soukromí (kompromitace citlivých údajů jako jedno z dopadových kritérií), práva na spravedlivé řízení (proces určování provozovatelů základních služeb) či práva nebýt dvakrát stíhán či trestán (správní řízení o porušení povinností podle zákona o kybernetické bezpečnosti v kontrapozici proti trestněprávní odpovědnosti). Navrhovaná úprava však nejenže nepředstavuje zásah do těchto práv či jejich nepřiměřené omezení, naopak v některých případech přispívá k jejich ochraně zajištěním adekvátní úrovně bezpečnosti informací tím, že realizuje zákonné zmocnění obsažené v účinném zákoně o kybernetické bezpečnosti.

V rámci mezinárodní spolupráce provedl NÚKIB sérii bilaterálních jednání určených k seznámení se s jednotlivými národními přístupy ke kritériím, které úřad provedl především během roku 2022.

Obsah tohoto návrhu vyhlášky nemá žádný vztah k obsahu nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA, o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013, tzv. „aktu o kybernetické bezpečnosti“.

Navrhované znění vyhlášky bere také v potaz obsah směrnice Evropského parlamentu a Rady o posílení kritických subjektů (tzv. směrnice CER).

Návrh vyhlášky je v souladu s obecnými zásadami práva Evropské unie, jako jsou např. zásada právní jistoty, proporcionality a zákaz diskriminace.

Návrh vyhlášky není v rozporu s judikaturou soudních orgánů Evropské unie a je v souladu s obecnými zásadami práva Evropské unie (např. zásadou právní jistoty, proporcionality a zákazem diskriminace).

Na základě těchto skutečností je možné návrh vyhlášky hodnotit jako plně slučitelný s právem Evropské unie.

d) Předpokládaný hospodářský a finanční dosah navrhované právní úpravy na veřejné rozpočty a dopad na podnikatelské prostředí České republiky

Vymezení hospodářských a finančních dopadů navrhované právní úpravy je součástí Závěrečné zprávy RIA v důvodové zprávě zpracované k Zákonu, který navrhovaná vyhláška provádí.

Obsah navrhované vyhlášky navazuje na ustanovení § X o prověřování rizik spojených s dodavatelem Zákona a z něho vyplývající mechanismus posuzování dodavatelů, jakožto složku s významným vlivem na stanovení hospodářského a finančního dosahu navrhované úpravy. Čím více dodavatelů bude omezeno, ať už formou varování či OOP, tím větší bude hospodářský či finanční dosah navrhované právní úpravy. Míra dopadu na podnikatelské prostředí se bude lišit v závislosti na počtu dodavatelů omezených NÚKIB.

Povinné osoby mechanismu jsou jak soukromoprávními, tak veřejnoprávními subjekty, přičemž jsou obě kategorie subjektů zastoupeny zhruba 50 % z odhadovaného počtu 150 povinných osob mechanismu. Nové povinnosti povinných osob mechanismu budou sestávat z povinnosti NÚKIB hlásit přímé dodavatele bezpečnostně relevantních dodávek, vynaložit přiměřené úsilí ke zjišťování nepřímých dodavatelů bezpečnostně relevantních dodávek a zjištěné nepřímé dodavatele taktéž hlásit NÚKIB. Tyto nové povinnosti generují na straně povinných osob mechanismu minimální administrativní náklady.

Potenciální významnější náklady povinným osobám mechanismu generuje povinnost dodržovat opatření vydaná NÚKIB. V případě upozornění na riziko spojené s dodavatelem se bude jednat o reflexi identifikované hrozby v analýze rizik, což je opět proces, který je u povinných osob mechanismu již nastavený a fungující. Případný zákaz dodavatele má potenciální vysoký dopad na povinné osoby. Pokud by povinná osoba identifikovaného zakázaného vysoce rizikového dodavatele využívala v bezpečnostně relevantní dodávce, bude muset takového dodavatele ze své infrastruktury vyloučit. Dle výsledků dotazníkového šetření[13] lze tedy předpokládat, že případné omezení dodávek dodavatele, které veřejné subjekty, které jsou zároveň povinnými osobami mechanismu využívají, toto omezení (popř. vyloučení) dodavatele bude znamenat zvýšené finanční náklady také pro veřejné rozpočty. Maximální

[13] Dotazníkové šetření bylo adresovaného všem orgánům a osobám dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti (odesláno prostřednictvím datové schránky 1. 11. 2022 s žádostí o sdílení vyplněného dotazníku do 30. 11. 2022). Následně NÚKIB vyhodnotil odpovědi orgánů a osob, které se stanou poskytovateli regulované služby v režimu vyšších povinností, kterým plynou povinnosti z mechanismu prověřování bezpečnosti dodavatelského řetězce, přičemž některé orgány či osoby spravující či provozující více systémů poskytli odpovědi za každý takový systém zvlášť. NÚKIB obdržel 65 takových odpovědí (dále jen „respondenti“).

náklady spojené s vyloučením významného dodavatele mohou být až ve výši[14] jednotek milionů Kč (3 % respondentů), desítek milionů Kč (34 % respondentů), stovek milionů Kč (16 % respondentů). 25 % respondentů uvedlo náklady vyšší než 1 miliarda Kč, nicméně náklady byly vyčísleny na takové výše z důvodu, že dané orgány či osoby uvažovaly o vyloučení dodavatelů, kteří jako jediní jsou schopni dané plnění poskytnout. Do kalkulace nákladů tak započítávali mj. dopady ukončení či omezení poskytování regulované služby, vč. ušlého zisku. Jelikož je dle navrhovaného mechanismu posuzování dodavatelů možné udělit výjimku z vyloučení dodavatele, a to v případě, pokud by mohlo být podstatným způsobem ohroženo poskytování regulované služby, takto vysoké náklady překladatel nepředpokládá. Vyloučení dodavatele ovšem může mít na povinnou osobu mechanismu při aplikaci přechodné lhůty odpovídající ekonomické životnosti aktiva také dopad nulový, jak uvedlo 22 % respondentů.

Přesnější vyčíslení nákladů není možné, protože do něj vstupuje řada neznámých proměnných, a to zejm. jak často bude nutné přistoupit k omezení některého z dodavatelů, v jakém rozsahu bude omezovaný dodavatel ve strategické infrastruktuře zastoupen a jaký způsob reakce na dané omezení přijme konkrétní povinná osoba mechanismu.

Další dopad na veřejné rozpočty závisí na pracovních kapacitách, které jednotlivé státní orgány zapojené do procesu posuzování rizik ze strany dodavatelů vyčlení na zmíněný proces a z toho vyplývající posuzování kritérií rizikovosti, uvedli v důvodové zprávě k zákonu o kybernetické bezpečnosti.

e) Předpokládané sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel; dopady na životní prostředí

Návrh vyhlášky je z hlediska sociálních dopadů a dopadů na specifické skupiny obyvatel neutrální. Zvýšení úrovně kybernetické bezpečnosti a tím pádem zajištění regulovaných služeb bude mít druhotný pozitivní dopad na společenské a ekonomické činnosti jako např. zajištění zdravotní péče či dodávky energie. Návrh vyhlášky je rovněž neutrální z hlediska dopadů na životní prostředí, lze však obdobně předpokládat pozitivní efekt v podobě předcházení takových bezpečnostních incidentů, které by negativní dopad mohly mít.

f) Zhodnocení současného stavu a dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Navrhovaná právní úprava je z hlediska zákazu diskriminace a z hlediska rovnosti mužů a žen neutrální.

g) Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů a dopadů na výkon státní statistické služby

Znění zákona o kybernetické bezpečnosti posiluje spolupráci mezi národními autoritami v oblasti kybernetické bezpečnosti i ochrany osobních údajů. Návrh vyhlášky je v ohledu ochrany osobních údajů bezrozporný, protože nestanoví žádné podmínky zásahu do ochrany osobních údajů. Druhotně může mít navrhovaná právní úprava pozitivní dopad na ochranu soukromí a osobních údajů, neboť rozšířením regulace v souladu s obsahem směrnice a tímto návrhem vyhlášky na nové subjekty dojde k rozšíření veřejnoprávní regulace kybernetické

[14] Na otázku uvedení maximálního finančního dopadu na zastupovanou organizaci v případě zákazu využívání plnění nejvýznamněji zastoupeného významného dodavatele dle § 2 písm. n) vyhlášky o kybernetické bezpečnosti po uplynutí ekonomické životnosti poskytovaného aktiva obdržel NÚKIB 32 odpovědí, které lze kvantifikovat.

bezpečnosti, která může mít z pohledu zavádění přiměřených organizačních a technických opatření kladný dopad také na ochranu osobních údajů v regulovaných organizacích.

Navrhovaná úprava nebude mít dopad na výkon státní statistické služby.

h) Zhodnocení korupčních rizik

Návrh zákona, a z toho vyplývajícího návrhu vyhlášky o kritériích posuzování rizikovosti dodavatele, může mít potenciálně zásadní dopady na poptávku po zboží a službách některých dodavatelů do strategicky významné infrastruktury ČR. Tato skutečnost může zapříčinit korupční tlak na změnu způsobu prověřování kritérií, výklad kritérií, určení samotných kritérií či úpravu celkového hodnocení rizikovosti dodavatele. Obdobně mohou i někteří správci regulované infrastruktury usilovat o to, aby nebyl konkrétní poskytovatel v důsledku posouzení rizikovosti omezen, jelikož by to pro ně znamenalo zvýšené náklady. Někteří správci mohou naopak usilovat o omezení konkrétního dodavatele za účelem zhoršení postavení svého konkurenta, který takového dodavatele využívá ve své infrastruktuře.

Jako pojistku proti možnému korupčnímu jednání vnímá předkladatel zejména to, že spolupráce na konkrétních případech prověřování dodavatelů bude probíhat v širokém okruhu na sobě nezávislých institucí, které budou poskytovat stanoviska a informace vycházející z vlastních zdrojů. Případné pochybení jedince by ve většině případů nemělo mít dopad na výsledek procesu.

V této souvislosti je rovněž vhodné upozornit na to, že osoby zapojené do fungování prověřovacího mechanismu budou zřejmě přicházet do kontaktu s utajovanými informacemi, a bude tedy nutné, aby byly držiteli adekvátního oprávnění pro přístup k utajovaným informacím. V rámci žádosti o vydání osvědčení a během doby, po kterou budou jeho držiteli, jsou povinny dokládat relevantní informace o svých majetkových poměrech

i) Zhodnocení dopadů na bezpečnost nebo obranu státu

Mechanismus posuzování dodavatelů a z toho vyplývající návrh vyhlášky zaměřený na kritéria posuzování rizikovosti dodavatelů bude mít pozitivní vliv na národní bezpečnost a obranu. Budování odolné strategicky významné infrastruktury bez rizikových dodavatelů značně přispěje její odolnosti. Právě odolná strategicky významná infrastruktura představuje klíčový faktor pro zajištění národní bezpečnosti a obrany. S tímto předpokladem pracuje jak aktuálně platná Bezpečnostní strategie ČR, tak i Národní strategie pro čelení hybridnímu působení a Národní strategie kybernetické bezpečnosti ČR. Vazbu na odolnou a bezpečnou infrastrukturu jako integrální součást národní bezpečnosti rovněž zdůrazňují strategické dokumenty NATO.

j) Konzultace

Podstatnou součástí procesu tvorby návrhu vyhlášky byla ze strany NÚKIB série bilaterálních jednání, zaměřená především na oslovení zástupců státních orgánů spolupracujících na přípravě Zákona, kterým tak byla dána možnost se k dané problematice vyjádřit již během příprav této právní úpravy před zahájením meziresortního připomínkového řízení. Proběhlo také vlastní šetření spočívající ve zkoumání a komparaci přístupů k dané problematice v zahraničí.

Podstatnou součástí procesu tvorby návrhu vyhlášky byla ze strany NÚKIB série bilaterálních jednání, zaměřená především na oslovení státních orgánů spolupracujících na

přípravě Zákona, dalších relevantních organizací a subjektů v rámci budoucích regulovaných odvětví. V rámci dotazníkového šetření pak byly osloveni také orgány a osoby dle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti. Výše uvedeným gestorům byly vždy minimálně zaslány teze vyhlášky a znění vyhlášky ve formě draftu s možností se vyjádřit k budoucí regulaci. Pokud tyto organizace na danou nabídku reagovaly, byl jim představen základ budoucí regulace dle aktuálního stavu.

NÚKIB také opakovaně vyzýval odbornou i širokou veřejnost k zasílání podnětů týkajících se budoucí regulace, a to především formou obecné výzvy na svých internetových stránkách. Veřejnost tak získala možnost svoje podněty k podobě vyhlášky Úřadu sdělit.

B. Zvláštní část

K § 1 – Předmět právní úpravy

Ustanovení vymezuje předmět regulace navrhované vyhlášky a odkázání na zmocňovací ustanovení Zákona, na základě kterého je podzákonný právní předpis vydáván. Současně je v ustanovení zavedeno několik zkratek, které se následně v normativním textu opakovaně vyskytují.

K § 2 – Země mající vliv na dodavatele

Předmětným ustanovením je definován pojem země mající vliv na dodavatele, tj. subjektu, který má možnost uplatňovat formální i neformální vliv na dodavatele. Přesné vymezení tohoto pojmu je nezbytné pro pochopení kritérií, jejichž převážná většina se zaměřuje na zemi mající vliv na dodavatele.

Cílem úpravy je obsáhnout veškeré myslitelné množiny zemí, se kterými má dodavatel natolik silný vztah, že jsou schopny jej účinně ovlivnit. Důraz je kladen na materiální pojetí vztahu, nikoli na formálně-právně aprobované skutečnosti, pro které by dodavatel mohl být ovlivněn, byť i tyto vazby nelze pominout. Pokud je cílem úpravy Mechanismu posuzování dodavatelů posílit bezpečnost České republiky, je nutné zohlednit a klást důraz na všechny relevantní myslitelné vazby států, které mohou na dodavatele působit. Je třeba akcentovat právě bezpečnostní hledisko a preventivní charakter Mechanismu posuzování dodavatelů. Potenciální nepřátelští aktéři budou podnikat kroky, jak zastřít svoje vazby na dodavatele, pročež se z povahy věci budou vyhýbat formálním a snadněji zjistitelným vazbám.

Shora uvedenou míru neformálnosti vztahu s dodavatelem sleduje i rozčlenění na jednotlivá písmena a) až e), kdy ustanovení nejprve operuje s pojmem formálního sídla a kaskádou dochází až k zcela neformálnímu uplatňování rozhodujícího vlivu bez ohledu na existenci právní skutečnosti, na základě které by takový vztah existoval.

Ad a)

Jedná se o nejformálnější formu vztahu, kdy se sídlem v tomto smyslu rozumí zapsané sídlo v příslušném veřejném rejstříku dané země. Země sídla dodavatele může mít zcela zásadní vliv na jeho jednání, ať už přímý (např. povinnost vytvářet politické orgány uvnitř organizace) či nepřímý (nastavení daňového systému). Současně se jedná o vztah, který lze nejkonkrétněji identifikovat, neboť vychází z právně aprobovaných a dostupných informací.

Ad b)

Lze předpokládat, že ve většině případů bude vůle dodavatele tvořena v zemi sídla. Nelze nicméně vyloučit, že dodavatel bude založen či přesídlen do jiné země, než ve které reálně vykonává svoji činnost, ať už z daňových či jiných důvodů. Proto je navrhováno vztáhnout kritéria i na země, kde je skutečně tvořena vůle dodavatele, a to ať už z důvodu, že jsou zde činěna významná manažerská rozhodnutí nebo se zde schází vedení dodavatele. Za jednání ve vztahu k řízení dodavatele se v tomto smyslu považují všechna manažerská rozhodnutí mimo běžnou provozní činnost. Jedná se však stále o formální řízení dodavatele, které vychází z jeho formalizované organizační a vlastnické struktury (např. rozhodnutí statutárního orgánu, jednatele, vedoucích manažerů apod.). Na osoby, které utváří vůli dodavatele mimo formalizovanou strukturu, cílí písm. c) a d) návrhu tohoto ustanovení. Návrh vytyčenou množinu formálního rozhodování v písm. b) dále omezuje pouze na země, kde jsou taková rozhodnutí činěna pravidelně. Pokud by takové omezení absentovalo, kritéria by se vztahovala i na nahodilé země, které by neměly reálný vztah k dodavateli.

Ad c)

Pro posouzení reálných vazeb dodavatele na konkrétní zemi je nezbytné, aby byla identifikována země, ve které pobývá osoba, jež v konečném důsledku vlastní nebo kontroluje dodavatele, tj. skutečný majitel. Pojem skutečný majitel je převzat ze zák. č. 37/2021 Sb., zákon o evidenci skutečných majitelů, kde je definován v § 2 písm. c). Skutečným majitelem může být pouze fyzická osoba, pročež je zjišťována země, kde má skutečný majitel faktický pobyt, nikoli sídlo podnikatele či registrovanou trvalou adresu. Touto cestou mohou být kritéria vztažena na zemi, kde skutečně pobývají osoby jež uplatňují rozhodující vliv na dodavatele, ale i příjemci zisku z jeho činnosti.

Ad d)

Definice přejímá rovněž pojem ovládání ve smyslu zák. č. 90/2012 Sb., zákon o obchodních korporacích. Dle § 74 odst. 1 uvedeného zákona je ovládající osobou ten, kdo může v obchodní korporaci přímo či nepřímo uplatňovat rozhodující vliv. Ovládání je nutno chápat ve smyslu možnosti opakovaného uplatňování vlivu, nikoli jednorázové možnosti. Současně se jedná pouze o možnost uplatnit vliv, nutně se nemusí jednat o vliv již uplatňovaný. Pro účely kritérií se jedná o podstatný institut částečně se prolínající s pojmem skutečný majitel v písm. c). Zák. č. 37/2021 Sb., o evidenci skutečných majitelů, rovněž užívá pojem „rozhodný vliv“ a přímo odkazuje i na úpravu v § 74 zák. č. 90/2012 Sb., zákon o obchodních korporacích [viz § 4 odst. 1 písm. d), odst. 2 zák. č. 37/2021 Sb., o evidenci skutečných majitelů].

Jak již bylo uvedeno, skutečným majitelem může být pouze fyzická osoba. Ovládající osobou dle § 74 odst. 1 zák. č. 90/2012 Sb., zákon o obchodních korporacích, může být ovšem kdokoli, včetně entity bez právní osobnosti. Z tohoto důvodu návrh ustanovení operuje s oběma pojmy – skutečný majitel v písm. c) a ovládající osoba v písm. d). Z důvodu snadnější interpretace je navržena zdvojená formulace v písm. d), která cílí na osoby (vazba na pobyt a sídlo) a na entity bez právní osobnosti (vazba na místo, odkud rozhodný vliv pramení).

Ad e)

Veškerá shora uvedená písmena navrženého ustanovení cílila na identifikaci země, se kterou je dodavatel nepřímo spojen (personálně a registrací sídla). Na základě písmene e) bude identifikována země, která na dodavatele působí přímo prostřednictvím státní moci. Současně stát může mít na dodavatele vliv i skrytě a bez nutnosti existence právní skutečnosti, na základě které by tak činil. Takto může jednat přímo či nepřímo prostřednictvím jiných osob.

V návrhu písm. e) jsou uvedeny složky vlivu státu na dodavatele: vyvíjení efektivního nátlaku, možnost rozhodujícího významného způsobu ovlivnění a uplatňování rozhodujícího vlivu.

Vyvíjení efektivního nátlaku se rozumí proti vůli dodavatele na něj efektivně působit bez ohledu na to, zda má nátlak požadovaný účinek. Efektivita nátlaku v tomto ohledu značí reálnou možnost státu, aby byl vliv účinný, tj. vliv musí splňovat určitý stupeň intenzity. V opačném případě by pod dané písmeno mohlo spadat nepřeberné množství států, které na dodavatele mohou působit prostřednictvím např. veřejných prohlášení.

Formulace možnosti rozhodujícího významného způsobu ovlivňovat je převzata z § 71 odst. 1 zák. č. 90/2012 Sb., zákon o obchodních korporacích, který upravuje institut ovlivnění. Návrh vyhlášky nicméně obsahově neodkazuje na tento institut, neboť ten je cílen na způsobení škody korporaci, nikoli na to, že by například způsobila škodu někomu jinému (navíc dodavatel nemusí být nutně korporací). Možnost rozhodujícího významného způsobu ovlivňovat značí jednorázový významný vliv na dodavatele, i nahodilý. Stejně jako v případě ovládání nezáleží

na tom, zda ke změně chování dodavatele dojde. Oproti ovlivnění je nicméně vyžadována vyšší intenzita vlivu ze strany státu.

Uplatňováním rozhodujícího vlivu se rozumí primární zdroj vůle, který určuje chování dodavatele. Stejná formulace se užívá v § 74 odst. 1 zák. č. 90/2012 Sb., zákon o obchodních korporacích (ovládání) a v § 4 a 5a zák. č. 37/2021 Sb., o evidenci skutečných majitelů (součástí konstrukce definice skutečného majitele). Rozhodující vliv má ten, kdo může přímo nebo nepřímo prostřednictvím jiné osoby nebo právního uspořádání dosáhnout toho, že rozhodování nejvyššího orgánu dodavatele odpovídá jeho vůli. Oproti rozhodujícímu významného způsobu ovlivnění se jedná o dlouhodobou kontrolu nad dodavatelem, nikoli nahodilou. Současně míra kvality vlivu je nižší oproti rozhodujícímu významnému způsobu ovlivňování. Podstatná je potencialita uplatnění rozhodného vlivu - fakticky k němu nikdy nemusí dojít.

K § 3 – Kritéria rizikovosti dodavatele

Navržené ustanovení shrnuje normativní důvod stanovení kritérií rizikovosti dle § X odst. 4 *[Prověřování rizik spojených s dodavatelem]* zákona. Důvodem je explicitní vyjádření důvodu i v rámci podzákonného právního předpisu. Současně ustanovení odkazuje na přílohu, kde jsou jednotlivá kritéria obsažena. Důvodem vyčlenění kritérií do samostatné přílohy je akcent na jejich přehlednost.

K § 4 – Způsob vyhodnocení kritérií rizikovosti dodavatele

Ustanovení upravuje způsob, jakým jsou kritéria rizikovosti vyhodnocována ve vztahu k naplnění jednotlivých kritérií navzájem, jakož i ve vztahu k jiným informacím zjištěných při prověřování rizik spojených s dodavatelem.

K § 5 – Účinnost

Návrh vyhlášky se váže k přijetí zákona o kybernetické bezpečnosti. Z toho důvodu je nezbytné stanovit termín nabytí účinnosti nejpozději k datu uvedenému v návrhu vyhlášky.

K Příloze – Kritéria rizikovosti dodavatele

Jedná se o přílohu, jejímž obsahem je tabulka s taxativním výčtem všech kritérií rizikovosti dodavatele. Kritéria pod čísly 1 až 8 jsou zaměřena na zemi mající vliv na dodavatele ,kdy cílí na otázky demokratického zřízení státu, povinnosti spolupracovat se zpravodajskými službami a uvalení mezinárodních sankcí na daný stát. Následující kritéria 9 až 13 se zaměřují již přímo na osobou dodavatele, konkrétně na jeho trestní minulost, podnikatelskou činnost, mezinárodní sankce a spolupráci se zpravodajskými službami.

Ad 1

Demokratický politický systém je založen na možnosti všech občanů vytvářet vůli státu (lid je zdrojem státní moci) prostřednictvím periodického procesu volby zástupců lidu ve vedení státu založeném na rovném, svobodném a všeobecném přístupu. Vyjádřením tohoto principu je aktivní a pasivní volební právo všech občanů. Základem demokratického zřízení je právo občanů sdružovat se do politických stran, hnutí a spolků a dalších sdružení, dále svoboda projevu a s tím spojené právo shromažďovací. Současně politická moc je v demokratickém státě z povahy věci dočasná.

Pro účely prověřování rizikovosti dodavatelů je dané kritérium podstatné, neboť v demokratickém právním státě, kde je periodicky redistribuována veřejná moc, je do značné míry umenšena možnost dlouhodobého působení státu na dodavatele. Osoby ve vedení státu

s demokratickým politickým systémem jsou zpravidla více omezeny v zásazích do přirozených práv člověka, včetně práva na majetek a s ním spojenou svobodu podnikání, neboť občané jim mohou v periodických volbách odebrat moc.

V případě, že bude zjištěno, že země mající vliv na dodavatele nemá demokratický politický systém, bude se jednat o indikátor rizikovosti dodavatele. Byť takový stát nutně nemusí zasahovat do práva na podnikání, panovalo by riziko, že představitelé státu k takovým zásahům mohou přistoupit, pokud absentuje či je významně umenšené riziko, že proti tomuto jednání budou občané protestovat či je nezvolí ve svobodných volbách.

Ad 2

Dělba veřejné moci, založená na principu brzd a rovnovah, je jedním z prvků demokratického právního státu, stejně jako shora uvedený politický systém. Veškerá moc státu by se měla sama vyvažovat striktním oddělením moci zákonodárné, výkonné a soudní tak, aby tyto složky veřejné moci nebyly ve stejných rukou a současně byly vytvořeny bariéry, které brání, aby jedna z mocí převážila nad oběma ostatními.

V rámci tohoto kritéria tak bude zkoumáno, zda v zemi mající vliv na dodavatele, existuje nezávislost soudů vázaných pouze zákonem, institut vyslovení důvěry vládě parlamentem apod. Pokud rozdělení mocí nebude v daném státě dostatečné či bude úplně absentovat, opět se bude jednat o indikaci možné rizikovosti dodavatele. Riziko poroste zejména při absenci nezávislého soudního přezkumu a možnosti domáhat se ochrany před nezákonným zásahem výkonné moci.

Ad 3

Dané kritérium se zaměřuje na kvalitu demokratického právního státu majícího vliv na dodavatele. Státní moc má být v právním státě vykonávána pouze dle pravidel stanovených prostřednictvím volených zástupců v právních předpisech určité právní síly – zákonech. Základním principem demokratického právního státu je vázanost státní moci zákonem, jak je stanoveno např. v čl. 2 odst. 3 Ústavy České republiky. Druhou stranou tohoto principu je svoboda jednotlivce činit vše, co není zákonem zakázáno.

Pro potřeby prověřování rizikovosti dodavatelů je kritérium podstatné z obdobných důvodů, jako dvě předchozí. Pokud státní moc země mající vliv na dodavatele není omezena zákonem, je do značné míry nepředvídatelné, co tato země může udělat, včetně možnosti zasáhnout do práva na podnikání osob, na které má země vliv.

Ad 4 a 5

Prostřednictvím zpravodajských služeb státy zpravidla provádí rozvědnou a kontrarozvědnou činnost utajovaným způsobem. Pomocí těchto služeb dochází k infiltraci, extrakci či likvidaci utajovaných informací, které mohou mít přímý vliv na bezpečnost cizího státu. Je proto nezbytné, aby v rámci kritérií byla vyhodnocena i tato oblast působení státu mající vliv na dodavatele.

V prvé řadě se jedná o vyhodnocení právní regulace zpravodajských služeb země mající vliv na dodavatele, konkrétně jakým způsobem povinuje jiné osoby ke spolupráci s těmito složkami státní moci.

Indikátorem rizikovosti bude zejména, pokud právní předpisy dané země stanoví povinnost:

1. spolupracovat se zpravodajskými službami nebo jinými bezpečnostními složkami země (např. v podobě povinnosti zaměstnávat či jinak zapojovat do svých podnikatelských procesů příslušníka zpravodajské služby nebo bezpečnostní složky),

2. sdílet data svého klienta s orgány veřejné moci země, zpravodajskou službou či třetími osobami, a to bez předchozího souhlasu státního zástupce nebo soudce,

3. upravit produkt, službu nebo proces poskytovaný dodavatelem dle pokynů orgánů veřejné moci, zpravodajské služby či třetí osoby.

Vzhledem k tomu, že povinnost spolupracovat se zpravodajskými službami je pravidelnou součástí právní regulace i států, které nebudou představovat rizikový faktor[15], je v navržené úpravě kritérium vztaženo pouze k zemím, kde plnění těchto povinností nelze přezkoumat nezávislým soudem, případně kde neexistuje soudní dohled nad těmito činnostmi zpravodajských služeb.

Pokud bude dané kritérium alespoň částečně naplněno, jedná se o podstatnou indikaci, že stát, který má vliv na dodavatele, má přímo možnost zjišťovat informace o aktivech kritických pro bezpečnost či stabilitu České republiky.

Následující kritérium cílí na stejné aktivity státu, nicméně se jedná o faktické vynucování spolupráce se zpravodajskými službami, bez nutnosti existence právní regulace. Za situace, že stát mající vliv na dodavatele takto skutečně jedná, je nutné považovat tuto skutečnost za velmi významný faktor rizikovosti dodavatele. Pro zjištění rizikovosti dodavatele je naplnění kritéria č. 5 významné, neboť stát jedná bez zákonného zmocnění, pročež nelze předvídat jeho jednání, včetně případné hostility k České republice a jejím spojencům.

Ad 6 a 7

Rizikovost dodavatele významně zvyšuje skutečnost, že země, která ně něj má vliv, má zaměřenou svoji kybernetickou strategii či doktrínu kybernetických operací proti České republice, jeho spojencům a významným mezinárodním uskupením, kterým je Česká republika členem. Nemusí se nutně jednat o explicitní strategii státu, ale i o seznam nepřátelských zemí, opakovanou formální atribuci kybernetických útoků vůči České republice a jejím spojencům apod.

Stejně tak je pro posouzení rizikovosti velmi významné, zda taková země vyvíjí obecně nepřátelské aktivity proti zájmům těchto subjektů.

Obě kritéria cílí na obdobné skutečnosti, tj. nepřátelské aktivity státu majícího vliv na dodavatele. Důvodem jejich rozlišení je zejména potřeba speciálně zohlednit kybernetické operace států (kritérium 6.), které o to více posilují riziko, že daný stát využije dodavatele k operacím zaměřeným proti České republice.

Ad 8

Pro posouzení rizikovosti dodavatele je podstatné vyhodnotit, zda na zemi mající na něj vliv byly uvaleny mezinárodní sankce. Navrhované kritérium pojmově odkazuje na § 2 zák. č. 69/2006 Sb., zákon o provádění mezinárodních sankcí, dle kterého se mezinárodními sankcemi rozumí *„příkaz, zákaz nebo omezení stanovené za účelem udržení nebo obnovení mezinárodního míru a bezpečnosti, boje proti terorismu, dodržování mezinárodního práva, ochrany lidských práv a svobod a podpory demokracie a právního státu, pokud vyplývá:*

a) z rozhodnutí Rady bezpečnosti Organizace spojených národů (dále jen "Rada bezpečnosti"), přijatých *podle článku 41 Charty Organizace spojených národů,*

b) ze společných *postojů, společných akcí nebo jiných opatření přijatých na základě ustanovení Smlouvy o Evropské unii o společné zahraniční a bezpečnostní politice,*

15 V České republice se jedná např. o povinnost součinnosti dle § 16c zák. č. 289/2005 Sb., zákon o Vojenském zpravodajství.

c) z přímo použitelných předpisů Evropských společenství, kterými se provádí společný postoj *nebo společná akce přijatá podle ustanovení Smlouvy o Evropské unii o společné zahraniční a bezpečnostní politice,*

d) z rozhodnutí přijatého na základě ustanovení Smlouvy o Evropské unii o společné zahraniční *a bezpečnostní politice, nebo*

e) z rozhodnutí *vlády, kterým dochází k zařazení na vnitrostátní sankční seznam podle sankčního zákona.“*

Účelem mezinárodních sankcí je udržení či obnova základních hodnot, na kterých stojí civilizované společenství států, od zajištění míru po ochranu lidských práv a svobod. Proto pokud byly zemi mající vliv na dodavatele uloženy mezinárodní sankce dle shora uvedené definice, jedná se významný indikátor rizika všech dodavatelů, na nichž má daná země vliv. Současně nelze pominout, že mezinárodní sankce se zpravidla dojednávají relativně dlouhou dobu, primárně z důvodu kombinace nastavení přesných podmínek a zájmů jednotlivých států. Samotný důvod uložení mezinárodní sankce je přitom často zcela zřejmý a bezrozporný. Navrhovaná úprava tuto skutečnost reflektuje, neboť kritérium lze naplnit i při vysoké pravděpodobnosti uložení mezinárodních sankcí. Typicky se bude jednat o situace, kdy se veškeré zainteresované subjekty dané mezinárodní platformy dohodly na nutnosti uložení mezinárodní sankce vůči předmětnému státu, ale dosud nejsou dojednány konkrétní parametry sankce (např. vymezení množiny produktů a služeb, na které se bude vztahovat zákaz dovozu).

Ad 9

Prvním kritériem vztaženým již přímo k osobě dodavatele, je existence pravomocného odsouzení dodavatele pro trestný čin. Tato skutečnost je základním identifikátorem pro důvěryhodnost dodavatele jako osoby. Navrhovaná úprava nicméně reflektuje, že ne každé odsouzení pro trestný čin bude dostatečně relevantní pro posouzení rizikovosti v rámci Mechanismu posuzování dodavatelů. Kritérium je proto omezeno pouze na určité množiny trestné činnosti (ve spojitosti s předmětem podnikání a významně ohrožující nebo porušující bezpečnost nebo vnitřní či veřejný pořádek).

Předmětem podnikání se v tomto smyslu míní jakékoli aktivity dodavatele, které směřují k dosažení zisku. Tyto činnosti nutně nemusí zahrnovat výhradně prodej kybernetických produktů a služeb, ale i veškeré další podnikatelské aktivity. Pro posouzení rizikovosti dodavatele je podstatné zjistit informaci o odsouzení ve všech těchto oblastech; pokud dodavatele byl schopen spáchat např. trestný čin podvodu podle § 209 trestního zákoníku ve spojení s podnikatelskou činností i mimo oblast informačních a komunikačních technologií, nelze důvodně vyloučit, že by byl schopen obdobnou činnost spáchat i v rámci bezpečnostně významných dodávek ve smyslu § X *[Prověřování rizik spojených s dodavatelem]* zákona.

Druhou množinou je trestná činnost, jež významně porušila či ohrozila bezpečnost České republiky, jejích spojenců a významných organizací, jejíchž je členem. Pokud účelem navrhované zákonné úpravy je zajištění bezpečnosti České republiky, je nezbytné zjistit, zda v minulosti již dodavatel nejednal způsobem, který by tuto bezpečnost ohrozil či porušil. Nejedná se nicméně o veškerá tato jednání, navržené kritérium je omezuje pouze na významné narušení či ohrožení, což reflektuje potřebu minimalizace zásahu v rámci Mechanismu posuzování dodavatelů.

Ad 10 a 11

Obě navržená kritéria zohledňují způsob výkonu podnikatelské činnosti dodavatele. Obě kritéria jsou velmi významná pro posouzení, zda je dodavatel důvěryhodný a zda je schopen stabilně a zodpovědně plnit bezpečnostně významné dodávky.

Rizikovost dodavatele významně zvyšují nekalostní jednání či praktiky v rámci relevantního trhu České republiky nebo jiných členských států Evropské unie, Evropského hospodářského prostoru, Severoatlantické aliance či Organizace pro hospodářskou spolupráci a rozvoj. Mezi tato nekalosoutěžní jednání lze především zařadit podplácení a klamavé označení zboží či služeb. Současně kritérium cílí na jakékoli nedovolené omezování hospodářské soutěže, ať už dohodami nebo spojením soutěžitelů či zneužitím dominantního postavení.

Pro posouzení rizikovosti dodavatele je nezbytné vyhodnotit i jeho podnikatelskou činnost, která nutně nevykazuje protisoutěžní charakter. Typicky se jedná o zjištění, zda jeho vedení jedná s péčí řádného hospodáře a je proto předpoklad ekonomické stability dodavatele. Obdobně, pokud budou zjištěny další skutečnosti, které svědčí např. o zadlužení a exekucích dodavatele, jedná se o indikátor rizikovosti dodavatele, jenž je třeba v rámci kritérií zohlednit.

Ad 12

Důvodem navrženého kritéria je reflektovat obdobné skutečnosti, jako je tomu v případě kritéria 8., tj. uvalení mezinárodních sankcí, nyní však přímo na dodavatele. V případě, že Česká republika či mezinárodní organizace uvedené v § 2 zák. č. 69/2006 Sb., zákon o provádění mezinárodních sankcí, uloží mezinárodní sankci dodavateli, jedná se o jednoznačný indikátor jeho rizikovosti s ohledem na principy a zásady, které mezinárodní sankce mají za cíl chránit.

Od 3. 1. 2023 je účinný zák. č. 1./2023 Sb., zákon o omezujících opatřeních proti některým závažným jednáním uplatňovaných v mezinárodních vztazích (sankční zákon), který nově zavádí možnost zařadit subjekt na vnitrostátní sankční seznam, a to z obdobných důvodů, jako je tomu v případě mezinárodních sankcí. Z tohoto důvodu kritérium bude naplněno i v případě zařazení na vnitrostátní sankční seznam.

Ad 13

Obdobně jako je tomu v případě kritérií 4. a 5., je zapotřebí vyhodnocovat vztah dodavatele a zpravodajských služeb států, které na něj mají vliv (blíže viz odůvodnění k těmto kritériím). Pokud dodavatel bude i bez existence právní povinnosti spolupracovat s těmito orgány sátu, jedná se o významnou skutečnost zvyšující jeho rizikovost. Míru naplnění bude určovat zejména intenzita spolupráce a její rozsah.