



PŘIPOMÍNKY

k materiálu Národního úřadu pro kybernetickou a informační bezpečnost

Návrh zákona o kybernetické bezpečnosti

V Praze dne 26. července 2023

Č. j.: 89/6000/2023

A. OBECNÉ PŘIPOMÍNKY

Národní úřad pro kybernetickou a informační bezpečnost (dále také jen „předkladatel“) předložil dne 19. 6. 2023 do elektronické knihovny legislativního procesu (dále také jen „eKLEP“) legislativní materiál – „Návrh zákona o kybernetické bezpečnosti“ (dále také jen „návrh ZKB“ nebo „materiál“).

Součástí návrhu ZKB je také mechanismus prověřování bezpečnosti dodavatelského řetězce (dále také jen „mechanismus“) v §§ 28-33 návrhu ZKB, který nad rámec transpozice směrnice NIS 2 přináší proces prověřování rizikovosti dodavatele, který v podobě uvedené v návrhu ZKB není proporcionální, představuje zvýšenou administrativní zátěž a zvýšené finanční náklady jak pro dodavatele, tak povinné subjekty, na které by měla navrhovaná právní úprava dopadnout, přičemž tyto dopady nejsou v rámci důvodové zprávy reflektovány a objektivně vyčísleny.

Návrh ZKB rovněž dává předkladateli pravomoci rozsahem i obsahem nepřiměřené jeho působnosti, v jejichž důsledku by předkladatel mohl zasahovat do otázek geopolitických (tedy oblasti náležející primárně do pravomoci vlády) a silně ovlivňovat hospodářskou soutěž. Návrh mechanismu tedy může negativně ovlivňovat podnikatelské prostředí jak na národní, tak mezinárodní úrovni, a zásadně zasahovat do svobody podnikání zaručené čl. 26 Listiny základních práv a svobod. Případné negativní dopady mechanismu lze tedy spatřovat jak na ekonomické, tak i geopolitické úrovni.

1.

Hospodářská komora ČR (dále jen „HK ČR“) se domnívá, že se předkladatel návrhu ZKB dostatečně nezabýval otázkou realizovatelnosti a dopadů navrhovaných opatření, protože rozsah a dopad povinností, ukládaných předloženým materiálem v důsledku zavedení mechanismu není proporcionální a zásadně přesahuje rámec působnosti předkladatele. Důsledkem mechanismu je zásadní dopad do ústavním pořádkem zaručeného práva podnikat, který se silně promítne jak v ekonomické, tak geopolitické rovině.

Připomínky předkládané níže k mechanismu prověřování bezpečnosti dodavatelského řetězce lze v obecné rovině rozdělit do 3 hlavních bodů:

1.1. Omezení rozsahu regulace na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni

Předkladatel opakovaně uvedl, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB však předkladatel vymezil rozsah mechanismu formou vyhlášky o nepominutelných funkcích, která mj. pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě), tak i v obecné rovině méně kritické části sítě (např. rádiová přístupová síť) nebo aktiva, která nemají přímý vliv na nedostupnost regulovaných služeb (jako je



např. fakturační systém). V návrhu ZKB také zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce.

V předkládaných připomínkách k návrhu ZKB níže HK ČR kritické části strategické infrastruktury transparentně rozdělila dle hrozeb a míry dopadu jejich realizace. Nejvýznamnější hrozbou je výpadek regulované služby. Rozsah mechanismu je tedy omezen na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro oblast telekomunikací se bude jednat zejména o jádro sítě, případně části přenosové sítě. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla dána možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifikuje významnou hrozbu.

Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval předkladatel. Předkladatel by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, přičemž poskytovateli strategicky významné služby by byla uložena povinnost ji každoročně aktualizovat.

Tento systém nazývá HK ČR tzv. kaskádou bezpečnostních povinností, kdy pro nejkritičtější část strategické infrastruktury bude povinnost řídit se případným omezením či zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána výslovná povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.

1.2. Zapojení vlády a sektorového regulátora do Mechanismu

a) zapojení vlády

Zákazem či omezením plnění dodavatele dochází k významnému zásahu do svobody podnikání mnoha subjektů na trhu. Zákaz i omezení plnění dodavatele může mít významné ekonomické, ale i geopolitické dopady. Obdobné dopady již stát v minulosti hodnotil v rámci právní úpravy prověřování zahraničních investic. V rámci procesu prověřování zahraničních investic dochází obdobně jako v případě mechanismu k prověřování osoby investora na základě strategických kritérií. Stejně jako v případě mechanismu může také dojít k zákazu investice. V případě prověřování zahraničních investic je zákaz investice podmíněn usnesením vlády. Stejně by tomu mělo být i v případě mechanismu, zejména s ohledem na skutečnost, že plošný zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice.

b) zapojení sektorového regulátora

HK ČR respektuje roli předkladatele v rámci procesu posouzení rizikovosti dodavatele, kterou by společně s vládou měl mít. V rámci určení lhůty pro implementaci případného omezení či zákazu plnění dodavatele je však role sektorového regulátora klíčová. Případné omezení či zákaz totiž může mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů (v případě telekomunikací jsou to například výstavbové povinnosti vyplývající ze zákona o elektronických komunikacích). Je tedy naprosto zásadní, aby daný sektorový regulátor (v případě telekomunikací ČTÚ), měl možnost se k implementaci omezení či zákazu vyjádřit a předkladatel musel k jeho stanovisku přihlídnout.

1.3. Kompenzace

Obdobně, jako tomu je v případě zákona o vojenském zpravodajství, navrhuje HK ČR do zákona zapracovat ustanovení o náhradě účelně vynaložených nákladů, které v návrhu ZKB zcela absentuje,



je však z hlediska dotčených subjektů zásadní. Konkrétní aspekty náhrady účelně vynaložených nákladů jsou popsány níže v návrhu nového ustanovení § 30a návrhu ZKB.

1.4. Začlenění klíčových ustanovení přímo do zákona

HK ČR navrhuje zapracování kritérií pro identifikaci regulované služby (§ 4), způsobu stanovení režimu poskytovatele regulované služby (§ 6 odst. 3), bezpečnostních opatření odpovídajících režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4), a kritérií pro identifikaci strategicky významné služby (§ 27 odst. 1) přímo zákonem. Zákonný legislativní proces poskytuje adresátům právní úpravy adekvátní míru stability regulačního prostředí i právní jistoty, která je nezbytná pro veškeré soukromé hospodářské aktivity. Zákonná úprava nadto ve smyslu Ústavy České republiky představuje projev vůle lidu skrze jeho řádně zvolené zástupce – vykonavatele zákonodárné moci. Tento způsob úpravy je vhodný pro řešení zásadních otázek regulace, mezi které bez jakékoliv pochybnosti patří i okruh regulovaných subjektů a stanovení jejich zásadních povinností. Naproti tomu úprava obsažená v předkládaném materiálu předpokládá, že otázka okruhu regulovaných subjektů – zejména poskytovatelů regulované služby a poskytovatelů strategicky významné služby – bude řešena pouhým prováděcím právním předpisem. Předkladatelem navrhovaný postup vnáší do otázky okruhu regulovaných subjektů a jejich klíčových povinností prvek volatility a nejistoty, která má z podstaty věci negativní dopad na hospodářskou činnost ve státě. Není navíc jasné, čím je odůvodněna zejména potřeba dynamicky a bez užití řádného zákonodárného procesu měnit okruh regulovaných subjektů.

2.

Ačkoli HK ČR vítá návrh zákona jako takový a jako včasnou implementaci Směrnice NIS 2, některá navržená ustanovení zákona mají potenciálně negativní dopad na digitální transformaci klíčových odvětví ekonomiky i státní správy. Zejména pak odvětví uvedená v § 27 návrhu (energetika, doprava a digitální infrastruktura a služby včetně telekomunikačních služeb) by na základě právní nejistoty spojené s povinnostmi strategicky významných služeb mohla ustupovat od digitalizace. Předkladatel počítá s vydáním metodického pokynu o rozsahu dostupnosti strategicky významné služby – provedení ale může být technicky nemožné (například spuštění pokročilých softwarových řešení, která mohou být součástí i kritické části, nemusí být v jiném data centru vůbec možná) nebo mohou ohrožovat obchodní tajemství („zálohové“ systémy mohou provozovatele data center a cloudových řešení nutit ke sdílení obchodních tajemství, nebo k vyhýbání se využití nejlepších možných prostředků digitalizace i v rámci základních řešení). Návrh zákona dále obsahuje nesoulad s transponovanou směrnicí NIS2 (viz konkrétní zásadní připomínky), který může mít negativní vliv na tržní prostředí.

3.

HK ČR oceňuje akceptování řady připomínek z veřejné konzultace a významné věcné úpravy návrhu zákona. Nadále však trvá na tom, aby většina povinností byla stanovena přímo v zákoně nikoli prostřednictvím prováděcích vyhlášek. Stejně tak trvá výhrada k nedostatečnému definování některých pojmů, u nichž bude přetrvávat aplikační nejistota.

Rovněž trvají výhrady k pravidlům hlášení kybernetických bezpečnostních incidentů (§ 16 a násl.). Není totiž zřejmé, zda je možné hlásit pouze významné incidenty nebo zda je nutné hlásit incidenty všechny. Lze se tudíž obávat významné administrativní náročnosti při aplikaci navržených pravidel. Metodická podpora NÚKIB bude zcela zásadní.

U neimplementační části zákona týkající se mechanismu prověřování bezpečnosti dodavatelského řetězce zásadní koncepční výhrady přetrvávají, přestože došlo k věcnému posunu oproti verzi zaslané k veřejné konzultaci. Zůstávají například nezodpovězené otázky v oblasti řešení vlastnické struktury dotčených dodavatelů nereflektující zejména existenci soukromoprávních smluvních vztahů mezi



poskytovateli regulovaných služeb a dodavateli (včetně možného uplatnění náhrady škod, sankcí atd.).

4.

Návrh zákona sice obsahuje důvodovou zprávu a závěrečnou zprávu RIA, ta ale neobsahuje měření administrativní zátěže podnikatelů dle platné metodiky Ministerstva průmyslu a obchodu z července 2017. Tato metodika je přitom závaznou pro zpracování RIA tak, jak to uvádí na svých stránkách Úřad vlády ČR. Metodika obsahuje vzorovou tabulku pro výpočet administrativní zátěže v právním předpise, kterou předkladatel zjevně nepoužil, aniž by zdůvodnil, proč. Stejně tak neodůvodnil, proč nepoužil výše zmíněnou metodiku.

Má-li právní předpis dopadnout na přibližně šest tisíc subjektů z podnikatelské i nepodnikatelské sféry, není možné dopad na ně shrnout větou, že „není z pohledu regulátora možné vyčíslit dopady na rozpočty v podobě absolutního čísla, které by bylo dostatečně přesné. Z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů.“ Předkladatel si mohl v průběhu zpracovávání návrhu zákona provést vlastní reprezentativní průzkum mezi potenciálními subjekty, případně si objednat studii od externího dodavatele, která by pomohla vyčíslit náklady a tak by byla zásadním vodítkem pro to, jak záměr předkladatele implementovat směrnici a do zákona vložit národní úpravu bezpečnosti dodavatelského řetězce řešit a jakým způsobem. Místo toho bohužel provedl „dotazníkové šetření“ adresované – jak píše v závěrečné zprávě RIA – orgánům a osobám podle § 3 c), d), f) a g) zákona o kybernetické bezpečnosti. To jsou ale v drtivé většině subjekty veřejné správy. NIS 2 přitom dopadne ve většině na subjekty ze soukromé sféry. Pokud úřad uvádí, že „z obdržených vyplněných dotazníků vyplýval extrémní rozptyl těchto předpokládaných nákladů“, pak je to důvod k provedení analýzy jiným způsobem, nikoli pouze k prostému konstatování toho, co se stalo.

HK ČR si dovoluje si upozornit, že například studie think tanku CETA pro Asociaci provozovatelů mobilních sítí odhaduje, že náklady jen v mobilní síti – pokud bude potřeba vyměnit dodavatele v celé části sítě – se mohou vyšplhat až k 17,8 miliardám korun. Není tak možné v Důvodové zprávě říci, že „výši finančních dopadů není možné předem stanovit“. Naopak, je potřeba vytvořit takový analytický podklad, který tyto náklady odhadne. (Shrnutí studie CETA je zde: <https://apms.cz/narodni-bezpecnost-chytre-za-stovky-milionu-tupe-i-za-18-mld/>). Už jen tato částka ukazuje, že dopad nového ZKB může být na podnikatelské prostředí extrémně významný a není možné jej v důvodové zprávě nechat nevyčíslený.

5.

Předkladatel uvádí, že součástí návrhu zákona je zavedení mechanismu prověřování bezpečnosti dodavatelského řetězce do českého právního řádu v souladu s usnesením Bezpečnostní rady státu ze dne 21. června 2022 č. 41. Usnesení ani zájem státu podobný mechanismus zavést HK ČR nijak nerozporuje. Zcela ale chybí jakýkoli analytický podklad, ze kterého by bylo patrné, z jakých dat předkladatel vychází a v jakém rozsahu je daný problém přítomný v České republice, tedy kolik potenciálně rizikových dodavatelů, na které by mechanismus dopadl, je přítomno v jakých částech infrastruktury subjektů, na které má mechanismus dopadnout. Dle zpráv z médií k podobnému kroku přistoupil například německý regulátor a ministerstvo vnitra, které mají na starosti regulaci kybernetické bezpečnosti. Předkladatel přitom v důvodové zprávě tvrdí:

„Nezřídkou se navíc stává, že identifikovaná hrozba, před níž Úřad vydal varování podle zákona o kybernetické bezpečnosti, není v analýze rizik povinných osob podle ZKB dostatečně, či dokonce jakkoli, reflektována.“

Přestože byla vodítka tohoto druhu ze strany správců této infrastruktury dlouhodobě požadována, k reflexi 5G Doporučení jeho adresáty po jeho vydání prakticky nedošlo; mnozí správci kritické



informační infrastruktury v sektoru elektronických komunikací nadále uzavírají kontrakty na dodávky technologií do bezpečnostně citlivých částí své infrastruktury s dodavateli, kteří po vyhodnocení kritérií 5G Doporučení na první pohled nevychází jako důvěryhodní.“

Tato tvrzení patří k části zdůvodnění toho, proč chce stát vůbec mechanismus zavést. Z tohoto textu z důvodové zprávy vyplývá, že předkladatel má zjevně z vlastní činnosti k dispozici analýzu reflexe Varování analýzu reflexe 5G Doporučení mezi povinnými subjekty. HK ČR požaduje, aby předkladatel doplnil do důvodové zprávy data z těchto analýz. Dále požaduje, aby předkladatel provedl naprosto základní analýzu současného stavu mezi potenciálními budoucími povinnými subjekty mechanismu, ze které vyplyne:

- Jaké dodavatele mají potenciální povinné subjekty v aktivech, u nichž ohodnotili dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická.
- Zda mají v praxi nasazenou mitigaci rizik spojených s dodavatelem, a případně jakou.
- Zda zohledňují rizika spojená s dodavatelem, která předkladatel identifikoval v tezích prováděcího právního předpisu a která zveřejnil v „5G Doporučení“.

HK ČR je přesvědčena, že bez úplně základní analýzy statu quo není možné přistupovat k jakékoli další regulaci, protože předkladatel vůbec nemůže mít informace o tom, jak jsou v současnosti tato rizika potenciálními povinnými subjekty vnímána ve světle jím vydaných opatření a materiálů, a případně mitigována. Pouze na základě podobné analýzy (a dalších analýz, které HK ČR zmiňuje výše) je možné přistoupit k vhodnému zvolení regulačního nástroje, který má dospět k zamýšlenému efektu při zohlednění zásad proporcionality. Nakonec i v legislativních pravidlech vlády se uvádí, že „přípravě každého právního předpisu musí předcházet podrobná analýza právního a skutkového stavu“.

6.

Některé subjekty na trhu elektronických komunikací jsou zároveň držiteli kmitočtových přidělů z aukcí kmitočtů z let 2017 a 2021. Podmínky spojené s přidělem kmitočtů představují například závazek velkoobchodní nabídky, závazek prioritního BB-PPDR, závazek národního roamingu pro PPDR, závazek pronájmu rádiových kmitočtů pro účely průmyslu 4.0, závazky týkající se pokrytí a podobně. HK ČR požaduje doplnit do důvodové zprávy ve spolupráci s ČTÚ předpokládaný vliv mechanismu na plnění těchto závazků.

B. ZÁSADNÍ KONKRÉTNÍ PŘIPOMÍNKY

1. Připomínka k § 1

HK ČR požaduje do § 1 návrhu doplnit nové odstavce 4) a 5) takto:

„(4) Aniž je dotčen mechanismus součinnosti podle § 60 a povinnosti k jmenování zástupce podle § 67, tento zákon se nevztahuje na osoby, které mají sídlo v jiném členském státě, s výjimkou:

- a) poskytovatele veřejně dostupné služby elektronických komunikací ^{*)},**
- b) osoby zajišťující veřejnou komunikační síť ^{*)} a**
- c) následující subjekty, jejichž hlavní provozovna ve smyslu odstavce 5 se nachází v České republice:**



1. *subjekt poskytující služby registrace jmen domén a poskytovatel regulované služby, který je poskytovatelem služby systému překladač jmen domén (DNS),*
2. *poskytovatel správy a provozu registru internetových domén nejvyšší úrovně,*
3. *poskytovatel služby cloud computingu,*
4. *poskytovatel služby datového centra,*
5. *poskytovatel služby sítě pro doručování obsahu (CDN),*
6. *poskytovatel služby on-line tržiště,*
7. *poskytovatel služby internetového vyhledávače,*
8. *poskytovatel služby platformy sociální sítě,*
9. *poskytovatel řízené služby (MSP), nebo*
10. *poskytovatele řízené bezpečnostní služby (MSSP).*

(5) *Pro účely tohoto zákona se má za to, že hlavní provozovna subjektu podle odst. 4 písm. b) v Evropské unii je umístěna v členském státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. Nelze-li takový členský stát určit, nebo nejsou-li tato rozhodnutí přijímána v Evropské unii, má se za to, že hlavní provozovna je v členském státě, v němž daný subjekt provádí činnosti k zajištění kybernetické bezpečnosti. Nelze-li takový členský stát určit, má se za to, že dotčený subjekt má hlavní provozovnu v členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Evropské unii.*

**) zákon č. 127/2005 Sb., o elektronických komunikacích “*

Odůvodnění:

Předložený návrh dle názoru HK ČR nedostatečným způsobem implementuje požadavky čl. 26 odst. 1 a 2 směrnice NIS 2.

Ačkoliv předkladatel připomínky k nedostatečné implementaci těchto ustanovení čl. 26 odst. 1 a 2 směrnice NIS 2 v rámci veřejné konzultace odmítl, vzhledem k potenciálním negativním dopadům nesprávné implementace na této připomínce HK ČR trvá a považuje ji za zásadní. Navrhuje proto důslednou implementaci tohoto mechanismu ve smyslu čl. 26 odst. 1 a 2 směrnice NIS 2.

V rámci vypořádání připomínek odkazoval předkladatel na ust. § 63 a § 67 návrhu zákona. Odkazovaná ustanovení § 63 a § 67 však implementují jen odstavce 3, 4 a 5 článku 26 směrnice NIS 2 a nijak nereflktují požadavky odst. 1 a 2, které představují tzv. one-stop-shop mechanismus, resp. tedy stanovují že některé subjekty (z povahy poskytovaných služeb) vždy budou podléhat jen jedné národní úpravě v rámci EU (nikoliv tedy jednotlivým národním úpravám v každém členském státě, kde je taková služba poskytována). Ačkoliv by bylo možné vykládat teritoriální aplikovatelnost zákona prostřednictvím přímé aplikace článku 26 směrnice NIS2, nepovažuje HK ČR takový postup za vhodnou legislativní techniku, jelikož může vyvolávat značnou právní nejistotu u adresátů tohoto zákona. HK ČR se domnívá, že vyjasnění aplikovatelnosti zákona žádným způsobem neomezuje princip součinnosti a zástupce ve smyslu odkazovaných ustanovení, která jsou ostatně přímo předvídána v čl. 26 odst. 3 až 5 směrnice NIS 2, a tudíž evropský zákonodárce předpokládal, že tato ustanovení budou existovat vedle sebe. Pro vyloučení pochybností o tom, že mechanismus součinnosti bude i nadále možné uplatňovat požaduje HK ČR doplnit výslovný odkaz.

Zároveň platí, že cílem návrhu zákona je implementovat směrnici NIS 2 (k tomu rovněž srov. § 1 odst. 2 návrhu zákona). Předložený návrh zákona nad rámec prosté implementace však obsahuje další

povinnosti, které nemusí mít ve směrnici jednoznačnou oporu – např. prověřování dodavatelského řetězce ve smyslu § 28 a násl. návrhu zákona nebo požadavky na zjištění dostupnosti strategicky významných služeb ve smyslu § 34 návrhu zákona. Ačkoliv směrnice NIS 2 vychází z principu minimální harmonizace (srov. čl. 5) a veškeré povinnosti v tomto zákoně by tak měly být vykládány eurokonformně a v mezích směrnice NIS 2, při aplikaci těchto specifických povinností nemusí být zjevné, že na poskytovatele usazené v jiných členských státech EU, se tyto specifické povinnosti neuplatní, a tedy že nepodléhají působnosti českého zákona o kybernetické bezpečnosti. Jinými slovy nemusí být zjevné, že v souladu s čl. 26 odst. 1 a 2 směrnice NIS 2 podléhají jen právní úpravě členského státu, ve kterém mají hlavní provozovnu.

V souladu s čl. 26 odstavce 1 a 2 směrnice NIS2 proto HK ČR považuje za klíčové vyjasnit na úrovni zákona, že český zákon o kybernetické bezpečnosti se neuplatní na vybrané subjekty, které jsou usazeny či mají hlavní provozovnu v jiném členském státě či v něm poskytují své služby, a proto podléhají právnímu řádu tohoto členského státu. HK ČR navrhuje stanovit, že zákon se nevztahuje na poskytovatele usazené v jiném členském státě, ledaže naplňují některou z výjimek stanovených v čl. 26 odst. 1 směrnice NIS 2, jak jsou navrženy implementovat do nového odstavce 4.

V souladu s čl. 26 směrnice NIS 2 se český zákon o kybernetické bezpečnosti tak uplatní pouze na:

- osoby sídlící v České republice, které naplní definici poskytovatele regulované služby (standardní teritoriální princip již implementovaný v návrhu zákona).
- poskytovatele veřejně dostupné služby elektronických komunikací, který v souladu se zákonem o elektronických komunikacích poskytuje služby na území České republiky (čl. 26 odst. 1 písm. a) směrnice NIS 2);
- osoby zajišťující veřejnou komunikační síť v souladu se zákonem o elektronických komunikacích na území České republiky (čl. 26 odst. 1 písm. a) směrnice NIS 2); a
- ty poskytovatele specifikovaných služeb, kteří mají hlavní provozovnu na území České republiky, požaduje HK ČR implementovat v odst. 4 písm. c) bodech 1 až 10 návrhu (čl. 26 odst. 1 písm. b) směrnice NIS 2).

Pro úplnost HK ČR uvádí, že obdobným způsobem byla z působnosti dosavadní směrnice „NIS 1“ (směrnice (EU) 2016/1148) vyňata aplikovatelnost na poskytovatele digitálních služeb. Pro srovnání:

Článek 26 odst. 1 směrnice NIS 2	Článek 18 odst. 1 směrnice NIS 1
Má se za to, že subjekty spadající do oblasti působnosti této směrnice podléhají pravomoci členského státu, v němž jsou usazeny, s výjimkou těchto případů: [....]	Pro účely této směrnice se má za to, že poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen. Má-li poskytovatel digitálních služeb v některém členském státě své sídlo, má se za to, že je v tomto členském státě rovněž primárně usazen.

Článek 18 odst. 1 směrnice NIS 1 byl přitom implementován ve stávajícím znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, následovně: „*Tento zákon se nevztahuje na poskytovatele digitálních služeb, který má sídlo v jiném členském státě.*“ (srov. § 33 odst. 4 zákona č. 181/2014 Sb.).



2. Připomínka k § 2

HK ČR ve vazbě na obsah § 28 odst. 3 písm. b) a nebude-li akceptována níže uvedená připomínka požadující vypuštění celého Dílu 5, požaduje, aby byl text § 2 upraven ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

HK ČR požaduje, aby v § 2 byly definovány všechny pojmy uvedené v § 28 odst. 3 písm. b), především pak bod 3, který není vymezen (definován) nijak. „Informační či komunikační služba“ je přitom extrémně vágní pojem, který je potřeba definovat zcela jasně. Nesplnění požadavků vyplývajících ze zákona s sebou nese vysoké riziko pokut, takže HK ČR předpokládá, že povinné subjekty by v rámci regulační opatrnosti předkladatele informovaly o všech dodavatelích, kteří se mohou být jen dotknout kritické části stanoveného rozsahu, mezi nimiž by při extenzivním výkladu pojmu „informační či komunikační služba“ mohly být třeba poskytovatelé služeb Public Relations (poskytují „komunikační“ služby managementu organizace, který může být „kritickou součástí stanoveného rozsahu“).

I při méně extenzivním výkladu pojmu „informační či komunikační služba“ může do těchto služeb spadat například pronájem nenasvíceného vlákna, jejichž riziko narušení bezpečnosti informací může být ohodnoceno na úroveň vysoká nebo kritická, ale nikoli z důvodů kyberútoku, ale fyzického přerušení, což ale vůbec nesouvisí s tím, kdo je dodavatelem onoho vlákna.

3. Připomínka k § 2 odst. 1 písm. a)

HK ČR požaduje upravit text takto:

„a) *aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování **nebo likvidace** informací a dat v elektronické podobě,*“

Odůvodnění:

Likvidace informací a dat je jednou z klíčových oblastí správy informačních aktiv.

4. Připomínka k § 2 odst. 1 písm. b)

HK ČR požaduje upravit text takto:

„b) *primárním aktivem informace a služby, přičemž informacemi se rozumí také data, včetně provozních a lokalizačních údajů, a službou se rozumí také procesy,*“

a současně požaduje v důvodové zprávě vymezit, o jaké procesy se jedná v případě služby.

Odůvodnění:

Vedle provozních údajů jsou lokalizační údaje důležitým atributem dat a informací. Navíc je zde vazba na zákon o elektronických komunikacích.

Jasně vymezení pojmu alespoň v důvodové zprávě pomůže aplikační praxi. Z textu návrhu není jasné, o jaké procesy se jedná, zda např. o procesy vedoucí k zajištění DDI regulované služby.

5. Připomínka k § 2 odst. 2 písm. f) a g)

HK ČR požaduje upravit definiční vymezení pojmu „kybernetický bezpečnostní incident“ ve vazbě na vyloučení úmyslného zavinění (např.: *kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv, s výjimkou případů, kdy lze s jistotou vyloučit úmyslné zavinění*), a to ve smyslu níže uvedeného odůvodnění.

Odůvodnění:



HK ČR rozumí, že poskytovatelé v režimu vyšších povinností nemají povinnost hlásit předkladateli tzv. provozní incidenty, které z povahy věci pod působnost předkladatele nespádají a incidenty, u kterých lze s jistotou vyloučit úmyslné zavinění a které nemají pro vyhodnocování ze strany předkladatele a další mapování bezpečnostní situace v kybernetickém prostoru zásadnější význam. Současně je definováno v § 16, odst. 1, že subjekty mají povinnost hlásit pouze incidenty, které vznikly v kyberprostoru. Tato znění vyčleňuje z povinnosti incidenty, které vznikly úmyslným zaviněním a případnou chybou samotného subjektu, např. při plánovaných pracích. Takto vyznívá i důvodová zpráva k návrhu zákona. V tomto smyslu by bylo tedy vhodné upravit formulace samotného pojmu „kybernetický bezpečnostní incident“.

NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s cílem ovlivnit jeho integritu nebo dostupnost nebo neoprávněný přístup nebo pokus o neoprávněný přístup k aktivu (systému) s cílem porušit jeho důvěrnost.

HK ČR doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu předkladatele: https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí:

Kybernetický bezpečnostní incident není potřeba Úřadu hlásit v případě, kdy došlo v důsledku technického selhání k nedostupnosti části aktiv, lze s jistotou vyloučit úmyslné zavinění (zejména útočníkem).

Zároveň HK ČR doporučuje vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů: „...a zároveň řádné zafungování k nim záložních (redundantních, zdvojených) aktiv zabránilo vzniku nedostupnosti systému jako celku.“ Cílem je hlášení incidentů, kde nelze vyloučit úmyslné zavinění bez ohledu na dostupnost.

6. Připomínka k § 2 odst. 2 písm. h)

HK ČR požaduje zpřesnit vymezení pojmu „významný dodavatel“ ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

Z hlediska aplikační praxe není uvedená definice jednoznačná a bude (podle názoru HK ČR) působit praktické problémy. Je tedy na místě požadovat, aby definiční vymezení významného dodavatele (jako účastníka „právního vztahu, který je významný z hlediska bezpečnosti informací ve stanoveném rozsahu řízení kybernetické bezpečnosti“, bylo výrazně návodnější.

7. Připomínka k § 3

HK ČR požaduje obsah § 3 přeformulovat tak, aby věcně kopíroval směrnici NIS 2 a stávající předpisy, a v souvislosti s tím doplnit důvodovou zprávu o příslušné vysvětlení, které nebude vyúsťovat v rozpor se směrnicí NIS 2.

Odůvodnění:

Článek 26 směrnice NIS 2 obsahuje zvláštní pravidla pro příslušnost a územní příslušnost. Ve vztahu k poskytovatelům služeb DNS, registrům názvů domén nejvyšší úrovně, subjektům poskytujícím služby registrace názvů domén, poskytovatelům služeb cloud computingu, poskytovatelům služeb datových center, poskytovatelům sítí pro doručování obsahu, poskytovatelům řízených služeb, poskytovatelům řízených bezpečnostních služeb, jakož i poskytovatelům on-line tržišť, on-line vyhledávačů nebo platforem služeb sociálních sítí (dále jen "poskytovatelé") stanoví čl. 26 odst. 1 písm. b) směrnice NIS 2 mechanismus jednoho správního místa, podle něhož poskytovatelé spadají do jurisdikce členského státu, v němž mají hlavní provozovnu v EU. Toto pravidlo je třeba vykládat tak, že poskytovatelé podléhají výlučně právu pouze jednoho členského státu a řídí se jím, i když poskytují služby v jiných členských státech. Současně čl. 26 odst. 5 směrnice NIS 2 stanoví povinnosti



vzájemné pomoci mezi orgány dohledu s pravomocí nad poskytovateli a orgány dohledu v jiných členských státech.

HK ČR se domnívá, že návrh zákona plně neprovádí mechanismus jednoho správního místa, jak je stanoven v článku 26 směrnice NIS 2. Konkrétně se jedná o čl. 26 odst. 5 směrnice NIS 2, který se provádí v § 54 návrhu zákona. Podle tohoto ustanovení má Agentura omezenou dozorovou pravomoc nad poskytovateli, kteří mají hlavní provozovnu v jiných členských státech než v České republice (dále jen "poskytovatelé z jiných členských států"). To potvrzuje i důvodová zpráva k § 54 návrhu zákona.

Čl. 26 odst. 1 písm. b) směrnice NIS 2 se však do návrhu zákona nenavrhuje implementovat v plném rozsahu. Podle důvodové zprávy k § 3 návrhu zákona se návrh zákona vztahuje na všechny poskytovatele regulovaných služeb usazené v České republice nebo poskytující služby do České republiky, a to včetně poskytovatelů z jiných členských států.

Ve vypořádání připomínek ze dne 10. března 2023 předkladatel reagoval na podobně formulovanou připomínku s tím, že tato úprava je v souladu s článkem 26 směrnice NIS 2 a navrhovaná úprava je nezbytná k zajištění toho, aby předkladatel měl požadovanou dozorovou pravomoc při poskytování součinnosti dozorovým orgánům s působností nad poskytovateli z jiných členských států. Takové vypořádání HK ČR nepovažuje za zcela správné, neboť nerozlišuje mezi: a) použitelností věcného předpisu a b) dozorovou pravomocí předkladatele. Konkrétně se jedná o následující:

- Návrh zákona se vztahuje na všechny poskytovatele regulovaných služeb usazené v České republice nebo poskytující služby do České republiky, tedy i na poskytovatele z jiných členských států. To znamená, že poskytovatelé z jiných členských států budou muset dodržovat veškerá nařízení podle návrhu zákona a návrhů aktů v přenesené pravomoci. To zároveň znamená, že i kdyby některý z poskytovatelů z jiných členských států jednal v souladu s hmotněprávní úpravou členského státu, v němž má hlavní provozovnu, ale nikoliv v souladu s hmotněprávní úpravou v České republice, jednalo by se o porušení českého práva.
- I když by takový poskytovatel z jiného členského státu pravděpodobně nebyl sankcionován vzhledem k omezené dozorové pravomoci předkladatele, stále by jednal protiprávně, což by mohlo představovat významný problém zejména pro poskytovatele služeb větším společenstvem a státním orgánům v České republice, kteří obvykle vyžadují plné dodržování všech právních povinností.

Na základě výše uvedených skutečností považuje HK ČR navrhované řešení za nevhodné a návrh zákona za rozporný se zamýšleným účelem směrnice NIS 2. Jak bylo uvedeno výše, navrhované řešení by vyžadovalo, aby subjekty splnily všechny platné povinnosti podle návrhu zákona a návrhů aktů v přenesené pravomoci.

HK ČR rovněž poznamenává, že navrhované řešení představuje podstatné rozšíření působnosti české právní úpravy kybernetické bezpečnosti. Ustanovení § 33 odst. 4 stávajícího zákona o kybernetické bezpečnosti výslovně stanoví, že se zákon o kybernetické bezpečnosti nevztahuje na poskytovatele digitálních služeb usazené v jiném členském státě.

8. Připomínka k § 4 odst. 1 a odst. 2

HK ČR požaduje upravit text § 4 v odst. 1 a 2 takto:

„(1) *Kritéria pro identifikaci regulované služby jsou tvořena kritériem služby a kritériem poskytovatele regulované služby. Kritéria pro identifikaci regulované služby stanoví ~~prováděcí právní předpis vlády~~ nařízením.*

(2) *~~Prováděcí právní předpis~~ **Nařízení vlády** stanoví kritéria pro identifikaci regulované služby v těchto odvětvích“*

Odůvodnění:



Původní znění umožňuje předkladateli, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v rámci vyjmenovaných odvětví. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná.

Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejprísnejší režim regulace dle zákona o kybernetické bezpečnosti.

9. Připomínka k § 6 odst. 3

HK ČR požaduje, aby byl text § 6 odst. 3 upraven takto:

*„(3) Režim poskytovatele regulované služby je stanoven ~~prováděcím právním předpisem~~ v **příloze tohoto zákona**. Je-li orgán nebo osoba poskytující regulovanou službu určen rozhodnutím Úřadu podle § 5, je vždy poskytovatelem regulované služby v režimu vyšších povinností.“*

Odůvodnění:

Požadavek reflektuje aplikaci principu právní a regulační jistoty.

10. Připomínka k § 9 odst. 1

HK ČR požaduje výslovně stanovit, že se za změnu považuje i výmaz, resp. ukončení regulované služby.

Alternativně HK ČR navrhuje nastavení podmínek a lhůty v § 11.

Odůvodnění:

Ustanovení § 9 odst. 1 nestanovuje, jak provést změnu registrace poskytovatele regulované služby směrem k podání oznámení výmazu (ukončení) regulované služby. Obecně § 9 řeší pouze registraci dalších služeb a změny režimu, avšak nezabývá se možností oznámení změn ve formě ukončení regulované služby. Navazující § 11 sice stanovuje postup výmazu z evidence poskytovatelů regulovaných služeb z pohledu předkladatele materiálu, ale nestanovuje proces (postup) podání oznámení změn z pohledu poskytovatele, pokud již nejsou plněna příslušná kritéria.

Cílem je umožnit, aby činnost, která odpadne, mohla být formálně ihned zrušena a poskytovateli nevznikaly další náklady.

11. Připomínka k § 10 odst. 2

HK ČR požaduje, aby byl text § 10 odst. 2 upraven takto:

*„(2) Poskytovatel regulované služby zapsaný v evidenci poskytovatelů regulovaných služeb je povinen plnit všechny povinnosti plynoucí mu ze zákona vůči zapsaným regulovaným službám **nejpozději od uplynutí šesti měsíců** od okamžiku doručení vyznění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyznění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11.“*

Odůvodnění:

Je třeba přijmout dostatečnou lhůtu k tomu, aby byl subjekt vůbec schopen plnit požadované povinnosti vyplývající ze zákona tak, aby obstál při případné kontrole. Z tezí vyhlášek vyplývá, že některé povinnosti budou poskytovatelé regulovaných služeb v režimu vyšších povinností muset realizovat pomocí zaměstnanců či kontraktorů s konkrétními znalostmi a dovednostmi, které nemusí být v dané organizaci dosud vůbec přítomny. Navíc musí dojít k revizi smluv s dodavateli a k další řadě plnění, které zajistí compliance. U menších poskytovatelů služeb elektronických komunikací



může být velká komplikace vůbec nalézt vhodné lidi – pokud se předpokládá, že po datu účinnosti zákona bude podobné subjekty poptávat velká část nově regulovaných subjektů, nemusí se na ně vůbec dostat. Je potřeba si uvědomit, že předkladatel bude regulovat nově až 2000 subjektů v odvětví elektronických komunikací, z nichž řada jsou mikropodniky v odlehlých venkovských oblastech.

12. Připomínka k § 12

HK ČR požaduje upravit text § 12 ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

Je na místě z požadovaných údajů vynechat ty údaje, které má předkladatel dostupné v základních registrech (tady je i vazba na prováděcí vyhlášku – například informace o vlastnické struktuře viz požadavek § 3 Vyhlášky o portálu NÚKIB). Portál NÚKIB by měl být napojen na základní registry, tudíž by registrační a doplňující údaje měly být z velké části, ne-li všechny, na těchto registrech dostupné.

13. Připomínka k § 13 odst. 3

HK ČR požaduje upravit text § 13 odst. 3 takto:

„(3) O provedení identifikace a určení organizačních částí a aktiv podle odstavce 1 vede poskytovatel regulované služby dokumentovaný záznam, a to včetně evidence primárních aktiv, která byla ze stanoveného rozsahu vyjmuta, a odůvodnění jejich vyjmutí.“

Odůvodnění:

Důvodová zpráva v prvním odstavci uvádí, že subjekty, které již nyní postupují podle platného a účinného zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti v procesu stanovování rozsahu řízení, budou mít situaci výrazně ulehčenou, jelikož nový postup pouze zpřesňuje již zavedenou praxi. Tuto tezi však vyvrací nová povinnost, kterou poskytovatelům ukládá právě § 13 v odst. 3, kde se nad rámec popsání a standardního procesu jednotlivých kroků identifikace nastavuje povinnost naprosto opačná, a to popsání a zdokumentování argumentace, proč daná aktiva nebyla zařazena.

V požadavcích návrhu nového zákona a prováděcích právních předpisů je však stanovena povinnost jasně popsat i předchozí kroky, které k zařazení aktiva vedou. Pro dokumentaci a doložení argumentů, proč dané aktivum nebylo zařazeno, tedy dostačuje interpretace popisu aktiva v předchozích krocích celého procesu. Popis nad rámec tohoto přináší administrativní zátěž subjektům a nepřináší přidanou hodnotu předkladateli.

14. Připomínka k § 14 odst. 1

HK ČR požaduje upravit text takto:

„(1) Bezpečnostními opatřeními se rozumí úkony, jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. ~~Bezpečnostními opatřeními jsou organizační a technická opatření.~~“

Odůvodnění:

Dle § 14 jsou bezpečnostními opatřeními organizační a technická opatření. HK ČR vnímá argumentaci předkladatele, že pro režim vyšších povinností jsou nastavena přísnější pravidla, zároveň není jasné, proč nelze – minimálně fakultativně – nastavit organizační a technická opatření i pro služby v režimu nižších povinností. V případě holdingu může totiž dojít k situaci, kdy některé společnosti spadnou do režimu vyšších a jiné do režimu nižších povinností. Zpravidla se však pro celý holding zpracovává jednotná řídicí dokumentace a bude poměrně náročně vést dvojkolejnou dokumentaci – organizační a technická opatření pro vyšší režim a bezpečnostní opatření pro režim



nižší. Ideální by bylo zachovat možnost stejného rozdělení pro oba režimy, ale věcný rozsah upravit dle typu režimu.

15. Připomínka k § 15 odst. 2 písm. c)

HK ČR požaduje upravit text takto:

„c) řízení **aktiv a rizik**,“

Odůvodnění:

Řízení rizik je možné pouze tehdy, jsou-li identifikována aktiva. Teprve po identifikaci aktiv lze definovat rizika. Teze prováděcích právních předpisů k navrhované právní úpravě řízení aktiv vůbec v nižším režimu neupravují. Naopak vyhláška o bezpečnostních opatřeních poskytovatele služby v režimu vyšších povinností v § 8 výslovně stanoví řízení aktiv a v § 9 řízení rizik. Původní návrh právní úpravy, který NÚKIB předložil k veřejné konzultaci (dokument 1a str. 10 – odst. 3 písm. v) „řízení aktiv“ obsahoval. Pokud tedy nedojde k doplnění samostatného bodu týkajícího se řízení aktiv, navrhuje HK ČR spojení řízení aktiv a řízení rizik do jednoho bodu.

16. Připomínka k § 16

HK ČR požaduje znění návrhu zákona přizpůsobit znění a záměru NIS 2 a zachovat povinnosti pro subjekty, které odpovídají označení “essential” a “important” ve smyslu NIS 2. Jiná úprava by mohla být v rozporu s NIS 2 a vytvořit nerovnoměrné zatížení subjektů.

Odůvodnění:

Článek 23 směrnice NIS2 stanoví ohlašovací povinnosti základních a významných subjektů. Podle tohoto ustanovení musí základní a důležité subjekty hlásit každou událost, která má významný dopad na poskytování jejich služeb. Návrh zákona implementuje článek 23 směrnice NIS 2 ve svém § 16. V porovnání se směrnicí NIS 2 stanoví § 16 návrhu zákona pro základní subjekty přísnější pravidla než pro významné subjekty. Podle tohoto ustanovení musí významné subjekty hlásit každou událost bez ohledu na její dopad na poskytování svých služeb.

Předkladatel v této souvislosti odkazuje na článek 5 směrnice NIS 2, který členským státům umožňuje přijmout nebo zachovat ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, pokud jsou tato ustanovení v souladu s právem EU. To potvrzuje i důvodová zpráva k § 16 návrhu zákona.

Předkladatel odůvodňuje tuto úpravu odkazem na stávající zákon o kybernetické bezpečnosti a uvádí, že takový přístup se v současné době uplatňuje. To HK ČR nepokládá za zcela vypovídající. Ustanovení § 8 zákona o kybernetické bezpečnosti rozlišuje oznamovací povinnosti většiny regulovaných subjektů a dále pak poskytovatelů digitálních služeb. Poskytovatelé digitálních služeb hlásí pouze takový incident, který má významný dopad na poskytování jejich služeb.

Na základě výše uvedeného a s ohledem na nové rozlišení podstatných a významných subjektů by se na poskytovatele cloudových služeb mohla vztahovat mnohem přísnější pravidla ve srovnání se současným stavem, neboť by mohli být považováni rovněž za podstatné subjekty.

17. Připomínka k § 17 odst. 3 a 5

HK ČR požaduje doplnit náležitosti závěrečné zprávy buď přímo do textu zákona (nebo alternativně do § 3 Vyhlášky o Portálu NÚKIB), tzn. upravit text § 17 odst. 3 a 5 ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

Připomínkované ustanovení ukládá poskytovatelům regulované služby povinnost do 30 dní od oznámení incidentu nebo předložení zprávy o aktuálním stavu zvládnutí kybernetického



bezpečnostního incidentu předložit závěrečnou zprávu, jejíž náležitosti mají být dle odst. 5 stanoveny prováděcím předpisem.

Vyhláška o Portálu NÚKIB se ale v § 3, který popisuje obsahové náležitosti úkonů spojených s hlášením kybernetických bezpečnostních incidentů, nevěnuje konkrétním náležitostem závěrečné zprávy, nýbrž pouze popisu obsahu formuláře pro hlášení incidentů, z něhož vyplývá, že slouží primárně k oznamování incidentů podle § 17 odst. 1 písm. a) nebo c) podávání průběžné zprávy o podstatných změnách stavu zvládnutí kybernetického bezpečnostního incidentu podle § 17 odst. 3 písm. b) zákona.

HK ČR proto požaduje doplnit obsahové náležitosti závěrečné zprávy tak, aby se předešlo nejistotě regulovaných osob ohledně způsobu plnění povinností podle § 17 odst. 1 písm. b) a c), obzvláště vzhledem k tomu, že za jejich porušení hrozí dle § 58 odst. 1 písm. h) ve spojení s odst. 15 písm. a) pokuta ve výši až 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obrátu.

18. Připomínka k § 19 odst. 1

HK ČR požaduje upravit text § 19 odst. 1 takto:

*„(1) Pokud to poskytovatel regulované služby považuje za vhodné, oznámí bez zbytečného odkladu uživatelům regulované služby kybernetický bezpečnostní incident s významným dopadem, který by mohl negativně ovlivnit poskytování této služby. Úřad je **po konzultaci s dotčeným poskytovatelem regulované služby** oprávněn uložit poskytovateli regulované služby, který je dotčen kybernetickým bezpečnostním incidentem s významným dopadem, povinnost informovat uživatele regulované služby o tomto incidentu. V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti. **Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.**“*

Odůvodnění:

V případě, že předkladatel uloží takovou povinnost bez předchozí konzultace, může dojít k poskytnutí informací, které takový incident mohou prohloubit, případně i vyvolat další incidenty s využitím informací získaných zveřejněním zranitelností.

Rozsah informační povinnosti není nijak upřesněn/omezen. Předkladatel tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.

19. Připomínka k § 19 odst. 2

HK ČR požaduje upravit text § 19 odst. 2 takto:

*„(2) Poskytovatel regulované služby, **který se dozví o významné kybernetické hrozbě ovlivňující jím poskytovanou regulovanou službu**, je povinen bez zbytečného odkladu **informovat Úřad, který vhodným a srozumitelným způsobem informuje** ovať uživatele regulované služby, který může být ovlivněn významnou kybernetickou hrozbou, o takových krocích, které může uživatel učinit v reakci na tuto hrozbu, aby byl případný dopad její realizace na tohoto uživatele co nejmenší. V případě, že je to možné a vhodné, informuje poskytovatel regulované služby uživatele také o této významné kybernetické hrozbě.“*

Případně variantně požaduje HK ČR alespoň ujištění o tom, že informace předávané poskytovatelem jsou generické informace podávané subjektům čelícím významné kybernetické hrozbě.

Odůvodnění:

Z navrhovaného znění zákona není patrné, o jakých hrozbách by měl poskytovatel regulované služby uživatele informovat a zároveň je povinnost stanovena nezávisle na vědomosti poskytovatele o



existenci hrozby. Povinnost je přitom spojena s nejvyšší možnou pokutou dle § 58 odst. 1 písm. k) ve spojení s odst. 15 písm. a).

HK ČR proto navrhuje jasně definovat, že poskytovatel je povinen informovat pouze o hrozbách, o kterých se dozví a které ovlivňují jím poskytovanou regulovanou službu. Dle navrhovaného znění by totiž bylo možné sankcionovat jakéhokoli poskytovatele za jakoukoli významnou hrozbu nezávisle na tom, jestli se hrozba dotýká jím poskytované regulované služby a jestli o hrozbě poskytovatel věděl nebo vědět měl.

Informace o významné kybernetické hrozbě by měl poskytovatel regulované služby předávat předkladateli, který agregovaně předá informaci širokému spektru subjektů, aby tak nedocházelo k přílišnému zahlcení kapacit řešitelských týmů poskytovatele regulované služby při nutnosti podávání individualizované informace o způsobu předcházení takové hrozbě jednotlivým subjektům. Tyto kapacity pak může poskytovatel využít pro řešení případné hrozby a dalším úkonům potřebným k udržení nejvyšší úrovně kybernetické ochrany.

20. Připomínka k celému Dílu 3 Vztah poskytovatele regulované služby a jeho dodavatelů

HK ČR požaduje doplnit příslušná ustanovení zavazující určeného dodavatele k součinnosti při plnění zákonných požadavků poté, co byl prokazatelně informován, že se stává osobou zajišťující bezpečnostně významnou dodávku strategické služby, a to ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

Dodavatel by měl mít v zákoně výslovně stanovenou povinnost spolupracovat. V praxi totiž bez součinnosti dodavatele, pokud tomuto není povinnost součinnosti textem právního předpisu výslovně uložena, nemusí být poskytovatel regulované služby schopen plnit zákonné požadavky.

21. Připomínka k § 21 odst. 1

HK ČR požaduje, aby byl text § 21 odst. 1 upraven takto:

*„(1) Úřad je po konzultaci s dotčeným poskytovatelem regulované služby z důvodu ochrany vnitřního či veřejného pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o **významném** kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému poskytovateli regulované služby rozhodnutím uložit, aby tak učinil sám. **Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby.**“*

Odůvodnění:

Směrnice NIS 2 v článku 23 odst. 7, ze kterého vychází § 21 „Výstraha“, pojednává pouze o „významných“ incidentech, toto zúžení ale v § 21 chybí, HK ČR požaduje jej doplnit. Jinak je oprávnění předkladatele informovat o kyberbezpečnostních incidentech prakticky bezbřehé.

Zveřejnění klasifikovaných informací a případného nesouladu s tímto zákonem může vést k narušení bezpečnosti informací a samotného smyslu zákona zajistit bezpečnost regulovaných služeb.

22. Připomínka k § 22 odst. 2

HK ČR požaduje, aby byl text § 22 odst. 2 vypuštěn a odst. 3 byl odpovídajícím způsobem přečíslován.

Odůvodnění:

Varování je instrument, který je v předkládaném návrhu upraven nad rámec směrnice NIS 2. V aktuálním znění zákona je varování (§ 12) upraveno tak, že jeho obsahem není nic ekvivalentního ve vztahu k odstavci 2. Jde tedy o typický gold-plating. V důvodové zprávě není nijak zdůvodněno, proč odstavec 2 předkladatel do § 22 vložil. Navíc pokud může předkladatel „stanovit jinak“, jak poskytovatel regulované služby v režimu vyšších povinností varování zohlední, znamená to významný



prostor k širokému zásahu předkladatele do svobody podnikání fakticky dle libosti. Předkladatel v důvodové zprávě správně píše, že „Varování je ve svém důsledku závazné pro poskytovatele regulovaných služeb v režimu vyšších povinností, jelikož ti v rámci svého systému řízení bezpečnosti informací a řízení rizik jsou schopni zohlednit hodnotu dané hrozby či zranitelnosti.“, pro existenci odstavce 2 tedy neexistuje žádný logický důvod.

Navrhovaný text dává předkladateli možnost prostřednictvím varování ukládat relativně blíže určenému okruhu osob povinnosti, které by adresát úpravy – zde poskytovatel regulované služby – byl bez dalšího povinen plnit. Vzhledem k okruhu adresátů, kteří by byli nuceni takto uložené povinnosti plnit, mohou být takové povinnosti ukládány přinejmenším formou opatření obecné povahy na základě zákonného zmocnění. Opatření obecné povahy je přitom ze zákona spojeno s procesními náležitostmi a prostředky procesní obrany, které v případě varování dle předloženého návrhu chybí. HK ČR má za to, že v předložené podobě je návrh co do otázky závazné povahy varování neústavní. HK ČR chápe potřebu předkladatele rychle a bez nadbytečných procedurálních formalit reagovat na vyvíjející se charakteristiky kybernetického prostředí a vhodným způsobem varovat soukromý sektor, nemůže se tak však díť formou ukládání závazných povinností.

23. Připomínka k § 23 odst. 5 a 6

HK ČR požaduje text § 23 odst. 5 a 6 upravit takto:

„(5) Opatření obecné povahy podle odstavce 4 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí poskytovatele regulované služby, kteří jsou jím dotčeni.

~~(6) Dotčený poskytovatel regulované služby či kdokoli, kdo prokáže, že jeho práva, povinnosti nebo zájmy mohou být opatřením obecné povahy přímo dotčeny, může k opatření obecné povahy vydanému podle odstavce 4 uplatnit připomínky ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.“~~

Odůvodnění:

Ustanovení odst. 6 připouští jen podání připomínek proti vydanému opatření obecné povahy, a to ve lhůtě 30 dnů. Připomínky jsou poněkud slabší nástroj ochrany ve vztahu k námitkám, o nichž je orgán vydávající opatření obecné povahy povinen samostatně rozhodnout, zrušením ustanovení se použije postup podle § 172 a násl. správního řádu, kde je možno uplatnit připomínky i námitky. Ve srovnání s připomínkami představují námitky procesně silnější nástroj ochrany práv.

Dále je potřeba uvést, že jen postup podle § 172 a násl. správního řádu je zárukou uplatnění práv, povinností nebo zájmu těch, kteří jsou opatřením obecné povahy přímo dotčeni, jelikož ustanovení § 173 odst. 2 správního řádu určuje, že proti opatření obecné povahy nelze podat opravný prostředek, kterým by subjekt mohl dosáhnout nápravy. Proti opatření obecné povahy nelze podat odvolání ani rozklad (na rozdíl od správního rozhodnutí).

24. Připomínka k § 24 odst. 2

HK ČR požaduje (alespoň) v důvodové zprávě upřesnit kritéria pro posouzení možnosti/nemožnosti zohlednění bezpečnostních požadavků.

Odůvodnění:

Jedná se o nový institut, proto by bylo vhodné koncipovat důvodovou zprávu podrobněji. Zejména jde o to, zda je poskytovatel regulované služby povinen splnit povinnosti i v případě značných nákladů.



25. Připomínka k § 25 odst. 1

HK ČR požaduje přeformulovat nebo upřesnit v § 25 odst. 1 slovní spojení „...hrozícího kybernetického bezpečnostního incidentu...“, a to ve smyslu níže uvedeného odůvodnění, a současně text § 25 odst. 1 upravit takto:

„(1) Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na podnět poskytovatele regulované služby v režimu vyšších povinností, který marně vyzval významného dodavatele ke splnění smluvního závazku předat informace a data, rozhodnutím uložit významnému dodavateli povinnost předat poskytovateli regulované služby v režimu vyšších povinností informace a data související s provozem aktiv sloužících k poskytování regulované služby. Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje nebo vzhledem ke skutkovým okolnostem není účelné po něm požadovat jejich opatření a vydání, může Úřad povinnost podle předchozí věty uložit i jinému orgánu nebo osobě, která požadovanými informacemi a daty disponuje. Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat. Rozhodnutí Úřadu o uložení povinnosti ohledně formátu, rozsahu, způsobu a lhůty předání informací podle předchozí věty nesmí jít nad rámec smluvních závazků jiného orgánu nebo osoby, jíž je povinnost ukládána.“

Odůvodnění:

Z díkce návrhu zákona není zřejmé, jakou metrikou bude vyhodnocována míra hrozby incidentu, která se nelehko kvantifikuje, pokud takový incident ještě nenastal. Není zřejmé, kdo určí, že se jedná o hrozící incident, a tedy oprávněnost žádosti. Není postaveno najisto, zda se jedná podle definice o Událost, není zřejmé, o jaká data a informace se jedná, pokud incident ještě nenastal. Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.

Ohledně formátu, rozsahu, způsobu a lhůty pro předání dat či informací je nutno respektovat smluvní ujednání.

26. Připomínka k Dílu 5 Mechanismus prověřování bezpečnosti dodavatelského řetězce

HK ČR požaduje, aby byl celý Díl 5 ze zákona vypuštěn a ze zákona odstraněny odkazy na ustanovení Dílu 5, případně alternativně,

aby schvalování mechanismu prověřování bezpečnosti dodavatelského řetězce mělo formu zvláštního zákonného předpisu mimo implementaci NIS 2.

Odůvodnění:

Mechanismus prověřování bezpečnosti dodavatelského řetězce s NIS 2 nijak zásadně věcně nesouvisí a není nutné ho schvalovat současně. Navíc na evropské úrovni se zjevně připravuje podobná právní úprava v podobě Telecoms Act, který avizoval v rozhovoru pro deník Les Echos evropský komisař pro vnitřní trh Thierry Breton (<https://www.lesechos.fr/tech-medias/hightech/thierry-breton-la-commission-soutient-les-etats-membres-qui-bannissent-huawei-1952702>). Je tak potřeba pečlivě zvážit (i s ohledem na další připomínky HK ČR), zda je vhodná forma prověřování dodavatelů čistě národní úprava a zda není vhodné postupovat na úrovni celé EU.

Zároveň samotná směrnice NIS 2 předpokládá celoevropské hodnocení dodavatelů v článku 22 „Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni“. Ten předpokládá, že Skupina pro spolupráci může ve spolupráci s Komisí a agenturou ENISA provést koordinované posouzení bezpečnostních rizik dodavatelských řetězců u specifických kritických služeb IKT, systémů IKT nebo produktů IKT, přičemž zohlední technické, případně netechnické



rizikové faktory. Dle našeho přesvědčení je vhodné postupovat v tomto ohledu na evropské a nikoli národní úrovni.

Předkladatel sám v důvodové zprávě uvádí (na straně 69), že kritéria jsou fakticky totožná, jaká navrhuje v mechanismu prověřování bezpečnosti dodavatelského řetězce. Navíc tvrdí, že v podobě § 23 má k dispozici nástroj (reaktivní protiopatření), kterým může povinným osobám nařídít zohlednění výsledků koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců:

„Reaktivní protiopatření je zároveň v této podobě i nástrojem odrážejícím požadavek, který směrnice NIS 2 na členské státy klade ve svém článku 21 odst. 3. Ten stanovuje členským státům povinnost disponovat nástrojem, prostřednictvím kterého zajistí, aby povinné osoby, tedy poskytovatelé regulovaných služeb museli zohlednit výsledky koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců podle čl. 22 směrnice NIS 2.“

Pokud má předkladatel k dispozici evropskou úpravu posouzení bezpečnostních rizik kritických dodavatelských řetězců fakticky se stejnými kritérii, jaké plánuje do národní úpravy, a nástroj, kterým dokáže donutit povinné osoby, aby zohlednily výsledky tohoto posouzení, pak je na místě otázka, k čemu je mechanismus na národní úrovni vlastně potřeba.

Pro případ, že by požadavek HK ČR na vypuštění celého Dílu 5 nebyl akceptován, požaduje HK ČR:

- detailní odůvodnění v důvodové zprávě a závěrečné zprávě RIA, proč se stát nerozhodl jít v tomto případě kroky, které předpokládá směrnice NIS 2. Ta v článku 22 kodifikuje přesně to, čeho chce stát dosáhnout vlastním mechanismem – tedy posouzení bezpečnosti rizik dodavatelských řetězců u specifických kritických služeb ICT, systémů ICT nebo produktů ICT, a to se zohledněním technických, případně netechnických faktorů. V souladu se zásadou proporcionality by měl předkladatel zdůvodnit, z jakého důvodu není toto ustanovení dostatečné a nevede k cíli, kterého chce stát dosáhnout. Je zcela legitimní otázka, zda článek není dostatečnou implementací mechanismu, jehož přípravu zadala předkladateli Bezpečnostní rada států ještě před tím, než bylo známo finální znění směrnice NIS 2, zvláště když předkladatel sám v důvodové zprávě tvrdí, že v podobě § 23 návrhu má k dispozici nástroj (reaktivní protiopatření), kterým může povinným osobám nařídít zohlednění výsledků koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců;
- koordinované posouzení rizik dodavatelských řetězců na evropské úrovni by dle pohledu HK ČR odstranilo mnoho nejasností, které jsou bohužel přítomné v současném návrhu. Protože dle článku 22 specifické služby, systémy a produkty ICT určí Komise po konzultaci se skupinou pro spolupráci a agenturou ENISA, nedojde k závažnému narušení jednotného trhu, kdy dnes reálně hrozí, že operátoři v jedné zemi (a v jedné podnikatelské skupině) budou moci využívat větší množství dodavatelů, než v zemi jiné. Tím se operátoři v zemi, kde stát úředně omezí množství dostupných dodavatelů, dostanou do konkurenční nevýhody, protože se jim logicky zvýší náklady – tím se stanou méně atraktivní pro potenciální investory a sníží se valuační jejich společností, což bude mít vliv na případný exit majitelů nebo na získání strategických investorů. Předkladatel by měl tyto aspekty zhodnotit podrobně v analýze RIA, kde zcela absentují;
- HK ČR upozorňuje, že existuje „Metodická pomůcka pro prevenci nadbytečné regulační zátěže při implementaci práva EU“ dostupná na stránkách Úřadu vlády ČR. Podle kapitoly II „Předcházení nadbytečné regulační zátěži při neminimalistické implementaci“ by měl předkladatel vždy posoudit, zda zvolená varianta implementace nepředstavuje nadbytečnou regulační zátěž a posouzení provést při hodnocení dopadů regulace. HK ČR požaduje, aby předkladatel dle této metodické pomůcky vyhodnotil, proč zvolil mechanismus prověřování



dodavatelského řetězce jako národní variantu a nikoli společný postup v rámci EU a jeho uplatnění na regulované subjekty v ČR pomocí § 23 návrhu;

- případné omezení dodavatelů významně ovlivní investiční kapacitu a schopnosti především menších a středních firem investovat do rozvoje svých sítí. Pokud budou NÚKIB nějakí dodavatelé omezeni nebo zakázáni, pochopitelně to sníží úroveň konkurence a zvýší ceny. Tento faktor musí NÚKIB zhodnotit v RIA v oddílu týkajícího se sociálních dopadů;
- předkladatel by měl také zhodnotit vliv na malé a střední podniky v RIA tak, jak to předpokládají příslušná pravidla.

27. Připomínka k § 28

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 upraven ve smyslu níže uvedeného odůvodnění a § 28 odst. 1 upraven takto:

„(1) Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele. Úřad využívá data výhradně za účelem vyhodnocování rizikovosti dodavatelů.“

Odůvodnění:

V kritériích rizikovosti dodavatele nejsou nijak zohledněna kritéria technické a organizační povahy zajišťování kybernetické bezpečnosti. Zahrnutí technických kritérií do hodnocení důvěryhodnosti dodavatelů byla přitom doporučena samotným předkladatelem v Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice z února 2022. Technické a organizační zajištění kybernetické bezpečnosti může být přitom vhodnou mitigací rizik vyplývajících ze „strategického“ posouzení dodavatele – minimálně by měl předkladatel a další orgány brát tato technická a organizační opatření v úvahu při rozhodování o rizikovosti dodavatele.

HK ČR tak požaduje doplnit do kritérií rizikovosti dodavatele technická a organizační kritéria a výslovně uvést do § 4 prováděcí vyhlášky (nebo přímo do zákona), že technická a organizační kritéria musí být brána v úvahu při vyhodnocování rizikovosti dodavatele a jako mitigační opatření.

Navrhované znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Navrhované znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout předkladateli na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.

HK ČR předepisuje, že navrhovaná úprava má vazbu i na změny v dikci § 29 odst. 3 – podrobnosti viz níže.

28. Připomínka k § 28 odst. 3 písm. a)

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 odst. 3 písm. a) upraven takto:

„a) kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úroveň vysoká nebo kritická a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby; kritickou částí stanoveného



~~rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem;~~

Odůvodnění:

Poskytovatelé strategicky významných služeb, kteří jsou povinnými osobami podle zákona č. 181/2014 Sb., mají klasifikovaná aktiva a u řady těchto aktiv může být dopad narušení bezpečnosti informací ohodnocen úrovní vysoká, aniž by přitom bylo přiměřené u těchto aktiv aplikovat mechanismus prověřování. Přijetí nového zákona přitom nebude odůvodňovat samo o sobě změnu hodnocení dopadu narušení bezpečnosti informací na tato aktiva. Je proto namístě aplikovat tento mechanismus pouze na aktiva s hodnocením dopadu úrovní kritická.

Omezení kritické části stanoveného rozsahu pouze na aktiva s hodnocením dopadu úrovní kritická přitom nevytváří riziko nedostatečného zahrnutí klíčových aktiv.

Předkladatel sám pojmenoval onu část stanoveného rozsahu, kterou chce prověřovat, jako „kritickou část stanoveného rozsahu“. Přitom aktiva, která mají být předmětem prověřování jejich dodavatelů, jsou taková, u kterých bylo ohodnocené poskytovatelem strategicky významné služby jejich případné ohrožení bezpečnosti informací na úrovni vysoká nebo kritická. Dle přesvědčení HK ČR postačí, když budou předmětem prověřování pouze aktiva, u nichž poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotí dopad narušení bezpečnosti informací na stanovených rozsah strategicky významné služby na úroveň kritická. Zároveň je HK ČR přesvědčena, že identifikace podle prováděcího právního předpisu postačuje k tomu, aby předkladatel dosáhl zamýšleného cíle, tedy že mechanismus bude prověřovat dodavatele aktiv, která jsou kritickou částí stanoveného rozsahu. Je to patrné i z toho, že v tezích vyhlášky jsou nepominutelné funkce stanovené pro sítě a služby elektronických komunikací, ale nikoli pro subjekty v ostatních odvětvích stanovených v § 27 odst. 1. HK ČR tak požaduje zrušit zákonné zmocnění předkladatele vydat prováděcí právní předpis stanovující nepominutelné funkce stanoveného rozsahu.

Rozsah mechanismu je navíc nutné zaměřit pouze na taková aktiva, u nichž má jejich nedostupnost přímý okamžitý dopad na nedostupnost strategicky významné služby, což je nejvýznamnější hrozba. Předkladatel by měl mít možnost zakázat rizikového dodavatele pro aktiva, jejichž výpadek může způsobit nedostupnost strategicky významné služby. Tento postup je s ohledem na princip proporcionality přiměřený.

Navrhované ustanovení ponechává pravomoc předkladatele provádět prověřování rizik spojených s dodavatelem tak, jak přepokládá materiál, odlišně však vymezuje některé pojmy spojené s touto pravomocí. Vzhledem k odlišné koncepci pojmu kritické části stanoveného rozsahu (viz níže), je obsolentním úkonem vydání vyhlášky o nepominutelných funkcích stanoveného rozsahu, jak předpokládá návrh ZKB, proto byla ze znění tohoto návrhu vypuštěna.

Pravomoc předkladatele má být realizována, v souladu s návrhem ZKB, prostřednictvím shromažďování a vyhodnocování informací, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele stanovených prováděcím právním předpisem, a které jsou spojeny s plněním konkrétního dodavatele. Kritéria rizikovosti dodavatele stanoví prováděcí právní předpis – vyhláška, k jejímuž vydání je zmocněn předkladatel v § 55 návrhu ZKB.

Jak uvádí předkladatel v důvodové zprávě k návrhu ZKB, cílem mechanismu prověřování bezpečnosti dodavatelského řetězce je umožnit státu identifikovat a vyhodnocovat hrozby spojené jak s orgány nebo osobami, které již jsou dodavateli do infrastruktury poskytovatelů strategicky významné služby, tak s orgány nebo osobami, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly, a to s cílem odhalit hrozbu ještě dříve, než bude u strategicky významné služby moci způsobit



narušení bezpečnosti informací. S ohledem na velké množství orgánů a osob, které mohou být předmětem prověřování, je stanovena možnost předkladatele prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů, tak jak to předpokládá i návrh ZKB, a to s ohledem na možná rizika a dostupné kapacity předkladatele.

Odstavec 3 předmětného ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem. Pojem „bezpečnostně významná dodávka“, který vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů, a „dodavatel bezpečnostně významné dodávky“, který vymezuje okruh orgánů a osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených, je dle tohoto návrhu shodný se zněním uvedeným v návrhu ZKB, proto se mu text zde nebude věnovat.

Změny však v tomto předkládaném návrhu doznal pojem „kritická část stanoveného rozsahu“, který vymezuje aktiva poskytovatele strategicky významné služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů.

Předkladatel opakovaně deklaroval, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB však předkladatel vymezil rozsah mechanismu formou vyhlášky o nepominutelných funkcích, která je výrazně širší, než bylo deklarováno, a například pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě – „core“), tak i méně kritické části sítě (jako je např. rádiová přístupová síť) nebo aktiva, která nemají přímý vliv na nedostupnost regulovaných služeb (např. fakturační systém). V návrhu ZKB i důvodové zprávě k němu zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce.

V předkládaném návrhu je stanovena nová úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby.

Předkládaný návrh vychází z předpokladu, že kritická část stanoveného rozsahu se skládá z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám v rámci plnění povinností podle § 13 návrhu ZKB ohodnotí dopad narušení bezpečnosti informací úrovní kritická.

Kritické části strategické infrastruktury jsou transparentně rozděleny dle úrovně hrozby a dopadů její případné realizace. Nejvýznamnější hrozbou je výpadek regulované služby – rozsah mechanismu tak byl v návrhu omezen výlučně na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro příklad – pro oblast telekomunikací se jedná zejména o jádro sítě, případně části přenosové sítě. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je přiměřené, aby byla dána možnost státu okamžitým zásahem omezit či zakázat vybraného dodavatele, u kterého identifikuje významnou hrozbu.

Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikuje předkladatel. Předkladatel by přitom (jako doposud) nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by měla být nově upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel strategicky významné služby měl povinnost každoročně aktualizovat (blíže viz odůvodnění § 30 návrhu níže).



29. Připomínka k § 28 odst. 3 písm. c)

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 odst. 3 písm. c) upraven takto:

„c) dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo ~~či jako poddodavatel~~ bezpečnostně významnou dodávku.“

Odůvodnění:

V současné podobě návrhu bude subjektem mechanismu prakticky každý lokální a regionální subjekt, který poskytuje provozovateli „kritické součásti stanoveného rozsahu“ velkoobchodně jakoukoli bezpečnostně významnou dodávku podle § 28 odst. 3 písm. b), což je ale fakticky jakákoli služba, protože předkladatel definuje aktiva natolik široce, že „kritickou částí stanoveného rozsahu“ je podle návrhu fakticky celá síť poskytovatele sítě či služby elektronických komunikací. Důsledkem toho je, že mechanismus nedopadne jen na subjekty, u kterých to předkladatel dle důvodové zprávy předpokládá, ale na stovky dalších subjektů. Předkladatel nebere v úvahu fakt, že sektor elektronických komunikací je extrémně propojen řadou dodavatelsko-odběratelských vztahů. Protože předkladatel definuje mechanismus extrémně široce fakticky jako celou síť, budou regulovanými subjekty i stovky malých a středních regionálních a lokálních operátorů, kteří poskytují velkoobchodní služby velkým národním operátorům. Zjevně jim neposkytují „kritickou“ službu (typicky pronájem vlákna či propoj základnové stanice s nějakým koncentračním bodem), ale přesto budou předmětem tlaku na změnu dodavatele od svých větších obchodních partnerů, protože budou součástí „kritické části stanoveného rozsahu“. To bude mít zásadní vliv na podnikání malých a středních regionálních firem, který není zohledněn v RIA (která má dle obecných zásad pro hodnocení dopadů regulace hodnotit dopad na podnikatelské prostředí „zejména s ohledem na osoby samostatně výdělečně činné a malé a střední podniky“).

Ostatně i z tohoto důvodu HK ČR požaduje změnit § 28 odst. 3 písm. a) skutečně jen na kritické části sítě, jak je uvedeno v předcházející připomínce.

Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou poskytovatelé strategicky významných služeb povinni zjišťovat informace dle § 32 odst. 1 písm. a).

V souladu s cílem a účelem předmětné úpravy je přiměřené, aby poskytovatel strategicky významné služby zjišťoval informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobcí daného produktu nebo poskytovateli služby ve vztahu, ke kterým je stěžejní prověřit rizikovost.

Navrhované znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licenci), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnost pro poskytovatele strategicky významných služeb by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby.

Taková hloubka prověřování by naopak byla přiměřená v případě služeb elektronických komunikací, kde by poskytovatelé strategicky významných služeb měli zjišťovat informace o dodavatelích použité infrastruktury, jakožto bezpečnostně významných dodavatelích, přičemž by měli promítnout opatření obecné povahy spočívající v zákazu nebo stanovení podmínek využívání plnění bezpečnostně významného dodavatele i na dodavatele infrastruktury pro využívané služby elektronických komunikací.

Vypořádání připomínky z veřejné konzultace se nevyrovnává s různorodou povahou poddodavatelů pospanou výše (dodavatele software vs. komponent). Ze skutečnosti, že hloubka prověřování musí



být přiměřená, neplyne možnost některé dodavatele, kteří nemají význam z hlediska kybernetické bezpečnosti, zcela ignorovat.

Touto úpravou se tento mechanismus omezí pouze na přímé dodavatele povinných osob, a nikoliv i dalších nepřímých poddodavatelů. Tímto zúžením počtu subjektů, na něž bude dopadat předmětná úprava, dojde k omezení této zásadní administrativní zátěže. Zároveň se předejde situaci, kdy např. povinnosti z předmětné úpravy budou muset plnit také dodavatelé poddodavatelů apod.

30. Přípomínka k § 28 odst. 4

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 28 odst. 4 vypuštěn z důvodů uvedených níže.

Odůvodnění:

Odůvodnění se částečně shoduje s odůvodněním uvedeným v připomínce k § 28 odst. 3 písm. a) a navíc je nutno zdůraznit, že navrhované znění zakládá právní nejistotu pro poskytovatele strategicky významných služeb i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se mohou v budoucnu významně a snadno změnit změnou vyhlášky. Navrhované znění v tomto směru pro obsah vyhlášky nestanoví žádné limity.

Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci, nesouladné s principem dělby moci, která je v demokratickém právním státě nezbytná.

Nelze přitom akceptovat vypořádání připomínky z veřejné konzultace, dle kterého je úprava kritérií formou podzákonného právního předpisu běžnou legislativní praxí. Podstata hodnocení bezpečnosti dodavatelského řetězce a dostupná opatření se závažností dopadu blíží opatřením podle zákona č. 34/2021 Sb. o prověřování zahraničních investic, přičemž zde jsou základní parametry hodnocení rovněž stanoveny zákonem. Současně již nyní navrhovaná kritéria jsou svou povahou obecná, lze proto očekávat minimum jejich změn. K jejich vyčlenění do prováděcího právního předpisu tedy není racionální důvod.

S ohledem na závažný ekonomický i provozní dopad na poskytovatele regulované služby tedy nelze akceptovat model, kdy by kritéria byla stanovena vyhláškou.

31. Přípomínka k § 29

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl v § 29 odst. 1 a 2 výčet orgánů, které jsou povinny poskytovat předkladateli informace a součinnost, rozšířen o Český telekomunikační úřad, případně obecné odvětvové regulátory, text § 29 odst. 3 vypuštěn (odst. 4 přečíslován na odst. 3), to vše ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

Zákon o kybernetické bezpečnosti a související předpisy významně dopadají na poskytovatele regulovaných služeb v oblasti služeb elektronických komunikací. Přesto navrhované znění výslovně nezmiňuje mezi orgány poskytujícími součinnost Český telekomunikační úřad (jakkoli jej lze považovat za „orgán“ podle odst. 3).

ČTÚ má přitom ve vztahu k oblasti služeb elektronických komunikací největší odbornost, dohlíží nad bezpečností a integritou komunikačních sítí a ukládá opatření k řešení hrozeb (§ 98 zákona č. 127/2005 Sb., o elektronických komunikacích), díky čemuž disponuje řadou informací významných z hlediska technologií, které je pro zajištění bezpečnosti dodavatelského řetězce třeba zohlednit (zejména z hlediska nepominutelných funkcí stanoveného rozsahu).



Navrhované znění explicitně neomezuje okruh dalších orgánů a osob, které jsou povinny poskytnout předkladateli informace a součinnost. To vytváří potenciál k zatížení povinných osob mechanismu prověřování dodatečnými povinnostmi k poskytování údajů, typicky v reakci na hlášení podle § 32 odst. 1 písm. b), a tak faktické rozšiřování výčtu údajů podle § 4 odst. 4 Vyhlášky o portálu NÚKIB.

Okruh osob a orgánů povinných k součinnosti vůči NÚKIB v této oblasti by měl být stanoven taxativně.

32. Připomínka k § 30

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 30 upraven takto:

„§ 30

Omezení rizik spojených s dodavatelem

- ~~(1) Úřad vydá opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby.~~
- ~~(2) Návrh opatření obecné povahy podle odstavce 1 Úřad po projednání s ostatními orgány uvedenými v § 29 odst. 1 a 2 a Ministerstvem financí předloží Bezpečnostní radě státu~~
- ~~a) pro informaci, jestliže lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy pro stávající či minulé plnění dodavatele bezpečnostně významné dodávky~~
- ~~1. je stanovena podle doby odpisování podle právního předpisu upravujícího zdanění příjmu⁴⁾, jestliže ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo~~
- ~~2. je alespoň 5 let, nebo~~
- ~~b) k projednání, jestliže lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy pro stávající či minulé plnění dodavatele bezpečnostně významné dodávky~~
- ~~1. není stanovena podle doby odpisování podle právního předpisu upravujícího zdanění příjmu⁴⁾, jestliže ji tento právní předpis ve vztahu k dotčené bezpečnostně významné dodávce stanoví, nebo~~
- ~~2. je kratší než 5 let.~~
- ~~(3) Po informování členů Bezpečnostní rady státu podle odstavce 2 písmene a) nebo po projednání podle odstavce 2 písm. b) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.~~
- ~~(4) Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 1. Zjistí-li Úřad, že tyto skutečnosti pominuly, zruší opatření obecné povahy podle odstavce 1 postupem podle odstavce 1 a 2 obdobně~~
- (1) Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání vládě České republiky (dále jen "vláda"). Před předložením věci vládě je Úřad povinen vyhotovit**



odhad nákladů povinných osob spojených se zavedením omezení či zákazu plnění dodavatele, který je nedílnou součástí dokumentace předkládané Vládě. Poskytovatel strategicky významné služby je povinen na výzvu poskytnout Úřadu potřebnou součinnost.

- (2) Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední soulad případného plnění dodavatele s principy demokratického právního státu, dopad na ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.
- (3) V návaznosti na usnesení Vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. Při stanovení podmínek dle předchozí věty je Úřad povinen přijmout vždy jen takové podmínky, které budou pro jejich adresáty nejméně zatěžující při zachování účelu odvrácení významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. K zákazu využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu může Úřad přistoupit jen tehdy, nelze-li významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku odvrátit pouhým stanovením podmínek dle věty prvé tohoto odstavce.
- (4) Usnesení Vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno.
- (5) Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad tak, aby tato lhůta byla pro poskytovatele strategicky významné služby nejméně zatěžující, při zachování účelu odvrácení významného ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele.
- (6) Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit.
- (7) Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pomínutí takové hrozby.
- (8) Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů, nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí.



- (9) *V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a).*
- (10) *Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok.*
- (11) *Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší.*
- (12) *Opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu lze vydat nejvýše na dobu v délce trvání tří let ode dne konce lhůty pro zohlednění podmínek nebo zákazu obsaženého v daném opatření obecné povahy.“*

Odůvodnění:

HK ČR je přesvědčena, že není možné, aby do procesu omezování dodavatele, což je fakticky velmi zásadní a závažný zásah do svobody podnikatelského prostředí, byl zapojen pouze předkladatel a ostatní státní orgány, především ty s politickou odpovědností, byly zapojené v procesu pouze okrajově poskytováním součinnosti či poskytováním informací.

Problematika mechanismu prověřování bezpečnosti dodavatelského řetězce už jde daleko za hranice kybernetické bezpečnosti, ale směřuje k obecnému prověřování hrozeb pro bezpečnost České republiky, její vnitřní a veřejný pořádek. V samotném návrhu se píše v § 28 odst. 1: “Úřad shromažďuje a vyhodnocuje informace a data spojené s orgánem či osobou, které se týkají možné hrozby pro bezpečnost České republiky, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovitosti dodavatele“. I kritéria pro hodnocení rizikovitosti dodavatelů určená ve vyhláškách se vůbec nezaměřují na kybernetickou bezpečnost, na technologie nebo služby, ale čistě na vyhodnocení právního a politického prostředí země mající vliv na dodavatele a na osobu dodavatele. Pro oblast vnitřního a veřejného pořádku a bezpečnosti České republiky je ústředním orgánem státní správy Ministerstvo vnitra. Problematika prověřování bezpečnosti dodavatelského řetězce se dotýká i pravomocí dalších ústředních orgánů státní správy – zahraničního obchodu, hospodářské soutěže, bezpečnosti a integrity služeb veřejných komunikačních sítí a služeb elektronických komunikací.

Omezení dodavatele je vysoce politickým krokem, který může mít zahraničněpolitické i ekonomické dopady, a spolurozhodovat by tak měly orgány s politickým mandátem. Do procesu posuzování dodavatele tak HK ČR požaduje (analogicky k zákonu o prověřování zahraničních investic) zapojit vládu (odstavec 1-4) a sektorové regulátory (odstavec 5-6)

Obdobně je tato problematika řešena na Slovensku v rámci § 27a odst. 3 zák. č. 69/2018 Z. z., o kybernetické bezpečnosti. Podle slovenské právní úpravy Národní bezpečnostní úřad Slovenska před vydáním rozhodnutí o omezení dodavatele, produktu, služby nebo procesu vyhotoví analýzu rizik na základě a v součinnosti s ostatními ústředními orgány státní správy, zpravodajskými službami a připraví návrh rozhodnutí. Návrh rozhodnutí potom předloží Bezpečnostní radě Slovenska a vládě. Od stanoviska vlády se potom Národní bezpečnostní úřad nemůže odchýlit. Navrhuje se řešit tuto problematiku v rámci českého návrhu zákona obdobně.

Navrhovaný § 30 obsahuje navíc další bezpečnostní opatření, kterými poskytovatel strategicky významné služby musí pro aktiva nezařazená jím do kritické části stanoveného rozsahu provést



analýzu rizik. V nich musí zohlednit rizika, která předkladatel uvedl v opatření obecné povahy a vypracovat plán zvládnutí rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem.

Jak je uvedeno ve zprávě o hodnocení dopadů, cílem prověřování rizik spojených s dodavatelem je minimalizace ekonomických dopadů a omezení pouze na kritickou část síťové infrastruktury. Pokud je cílem vymezit pouze kritickou část strategické infrastruktury, mělo by se jednat o aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifikuje významné hrozby. Pro zbylé části aktiv strategicky významné služby je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval regulátor. Regulátor by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel měl povinnost ročně aktualizovat.

Nově je navrženo zapojení Vlády ČR do procesu vydávání opatření obecné povahy. Je nezbytné, aby v případě vyhodnocování hrozeb měla vláda možnost posoudit dopady úkonů předkladatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obrany státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku.

Lhůtu plnění povinností poskytovatele z opatření obecné povahy je navrženo stanovovat na základě délky životního cyklu aktiv bezpečnostně významné dodávky, která je vyjádřena účetními odpisy jednotlivých aktiv. V případě, že je takové lhůta zkrácena, znalec stanoví výši náhrady.

Nový návrh ustanovení § 30 návrhu ZKB zakotvuje možnost omezit nebo zakázat využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, a to zjistí-li Úřad postupem podle § 28 odst. 1 návrhu ZKB, že může být významně ohrožena bezpečnost České republiky nebo vnitřní či veřejný pořádek.

Jak již bylo uvedeno, oproti návrhu ZKB je do procesu prověřování rizik spojených s dodavatelem zapojena vláda. Zapojení vlády v procesu prověřování rizikovosti dodavatele je zásadně smysluplné a důležité, a to jak z hlediska transparentnosti a objektivit rozhodování, tak vzhledem k závažnosti opatření obecné povahy, které na základě uvedeného ustanovení zákona může být vydáno. Případný zákaz či omezení plnění dodavatele musí vždy být až nejzazším řešením – představuje totiž značný zásah do ústavně zaručených práv a povinností jednotlivých subjektů, i proto musí být podmíněn právě usnesením vlády.

Je třeba podotknout, že vláda do jisté míry v současnosti již do posuzování rizikovosti dodavatele (resp. investora) zapojena je, a to dle zákona č. 34/2021 Sb., o prověřování zahraničních investic. Dle zákona o prověřování zahraničních investic jsou přijetím usnesení vlády podmíněna rozhodnutí omezující či zakazující zahraniční investici, a to právě s ohledem na míru zásahu do práv dotčených subjektů v důsledku tohoto omezení či zákazu. Začlenění vlády do procesu prověřování rizikovosti dodavatele má tedy pevné základy již v aktuálně účinné právní úpravě a rozhodnutí o omezení či zákazu plnění dodavatele by mělo být podmíněno usnesením vlády (obdobně jako u zahraničních investic), a to zejména s ohledem na to, že plošný zákaz či omezení plnění dodavatele může mít mnohem větší dopad na trh než zákaz doposud neuskutečněné investice.

Řešení otázky dodavatelského řetězce zasahuje do vícero oblastí, nejen do oblasti bezpečnostní. Pouze vláda může posoudit jak geopolitické a ekonomické dopady věci, tak i bezpečnostní aspekty – ostatně takto to činí již dle zákona o prověřování zahraničních investic, kdy vláda posuzuje, zda je



případné omezení či zákaz zahraniční investice nutný z důvodu ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku, přičemž při posuzování jsou hodnocena i strategická kritéria, jako je hodnocení investorů z hlediska země jejich původu (např. zda je zahraniční investor ovládán přímo či nepřímo vládou třetí země, či zda již byl zapojen do činností ovlivňujících bezpečnost nebo veřejný pořádek v některém členském státě EU). Právě z důvodu komplexnosti celé problematiky a přesahu do rozličných oblastí není vhodné, aby věc byla konzultována pouze s Bezpečnostní radou státu, jejímž předmětem činnosti je výhradně koordinace problematiky bezpečnosti České republiky, jak navrhuje návrh ZKB. Nadto je třeba uvést, že usnesení vlády jsou závazná zásadně širěji, než usnesení Bezpečnostní rady státu (usnesení vlády zavazují všechny členy vlády, ministerstva, jiné ústřední orgány státní správy, ostatní správní úřady a další subjekty, pokud tak stanoví zvláštní zákon, zatímco v případě usnesení Bezpečnostní rady státu je závazná pouze jeho ukládací část (jen v oblasti zajišťování bezpečnosti České republiky), a to pouze pro určené členy vlády a vedoucí jiných správních úřadů).

Vedle zapojení vlády počítá předkládaná připomínka rovněž s účastí sektorových regulátorů (příslušných ústředních orgánů státní správy), jejichž pozice je v návrhu ZKB značně opomíjena, je však v procesu prověřování zcela zásadní. Právě příslušní sektoroví regulátoři disponují potřebným penzem informací a odborných znalostí o fungování a činnosti daného regulovaného sektoru a jsou schopni posoudit reálné dopady případného omezení či zákazu plnění dodavatele, jakož i přesah do oblasti úpravy zajišťované zvláštními právními předpisy pro daný sektor (např. ohrožení plnění povinností subjektů stanovených těmito zvláštními právními předpisy).

V návaznosti na usnesení vlády a konzultaci se sektorovými regulátory, je dáována předkladateli pravomoc vydat konkrétní omezení formou opatření obecné povahy, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb. Toto opatření obecné povahy však musí být přijato na základě usnesení vlády a zohledňovat stanovisko příslušného sektorového regulátora.

S ohledem zákonnou nemožnost procesní obrany proti opatření obecné povahy po uplynutí lhůty jednoho roku od jeho vydání, navrhuje HK ČR limitovat trvání opatření obecné povahy na tři roky s tím, že v případě trvání důvodů, pro které bylo opatření vydáno, bude jeho obsah vydán ve formě nového opatření, které bude moci být opětovně přezkoumáno soudy.

Proces prověřování rizikovosti dodavatele je dle obsahu připomínky nastaven následovně:

Pokud předkladatel na základě vyhodnocení kritérií rizikovosti dospěje k závěru, že plnění dodavatele může představovat významné ohrožení bezpečnosti anebo vnitřního či vnějšího pořádku České republiky, předloží věc k projednání vládě.

Vzhledem k tomu, že možné opatření omezující či zakazující plnění konkrétního dodavatele může mít rozsáhlé dopady nejen na dodavatele samého, ale i na povinné osoby (poskytovatele strategicky významných služeb), jichž se opatření obecné povahy dotýká, bude předkladatel ještě před předložením věci vládě povinen vypracovat odhad nákladů spojených s implementací povinností stanovených v opatření obecné povahy povinnými osobami. Tento podklad je zásadní pro samotnou vládu, aby mohla věc posoudit ve všech souvislostech a učinit informované rozhodnutí s vědomím veškerých hrozících dopadů. Za účelem vypracování odhadu nákladů jsou poskytovatelé strategicky významné služby povinni předkladateli poskytnout potřebnou součinnost.

Vláda bude mít následně k dispozici lhůtu 45 dnů k projednání a vydání usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, přičemž při posuzování věci vláda zohledňuje jak možný dopad plnění dodavatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného



pořádku. Usnesení vlády bude pro předkladatele vždy závazné a bude jím podmíněno vydání zakazujícího či omezujícího opatření obecné povahy.

V návaznosti na usnesení vlády o tom, že plnění dodavatele představuje významné ohrožení, je předkladateli dávana pravomoc vydat opatření obecné povahy, kterým stanoví podmínky nebo zakáže plnění dodavatele bezpečnostně významné dodávky. Z povahy opatření obecné povahy vyplývá, že jde o opatření, kterým se budou muset řídit všichni poskytovatelé strategicky významných služeb – směřuje však vždy vůči vymezeným plněním daného dodavatele (proti bezpečnostně významné dodávce). Stejně jako v návrhu ZKB, se vydání opatření obecné povahy řídí obecnou právní úpravou obsaženou ve správním řádu, a to s výjimkou ustanovení, která pojmově nejsou přílehlavá k problematice prověřování rizikovitosti dodavatele (týkají se typicky nemovitostí a územního rozvoje). Z obecné právní úpravy také vyplývá možnost přezkoumat opatření obecné povahy v přezkumném řízení nebo v soudním řízení správním dle obecné úpravy správního řádu a správního řádu soudního, nelze však proti němu podat opravný prostředek.

V rámci omezujícího či zakazujícího opatření obecné povahy předkladatel vždy stanoví i přiměřenou lhůtu pro zohlednění podmínek či zákazu. Pozměněná úprava ukládá, že lhůta musí být vždy stanovena v návaznosti na projednání s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, neboť právě sektoroví regulátoři disponují objektivními informacemi, na jejichž základě lze přiměřenou lhůtu stanovit.

Je nutné trvat na tom, aby omezení či zákaz stanovený prostřednictvím opatření obecné povahy byly vždy proporcionální a přiměřené a nekolidovaly s právní úpravou obsaženou ve zvláštních právních předpisech. Vzhledem k tomu, že případné omezení či zákaz plnění dodavatele mohou mít významný dopad na schopnost povinných osob plnit své zákonné povinnosti vyplývající ze zvláštních právních předpisů, je za tímto účelem navrhováno, aby předkladatel projednal s příslušnými ústředními orgány státní správy (sektorovými regulátory), do jejichž působnosti náleží strategicky významná služba, do níž směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností uvedených ve zvláštních právních předpisech. Například pro oblast telekomunikací jde mj. o výstavbové povinnosti vyplývající ze zákona č. 127/2005 Sb. o elektronických komunikacích. Je tedy zásadní, aby daný sektorový regulátor, v tomto případě Český telekomunikační úřad, měl možnost se k implementaci omezení či zákazu vyjádřit a předkladatel musel k jeho stanovisku přihlídnout.

V souladu s návrhem ZKB je i v připomínce pozměněném návrhu zachována povinnost předkladatele pravidelně (nejméně jednou za 3 roky) přezkoumávat trvání skutečností, na jejichž základě bylo vydáno omezení či zákaz, aby byla v případě jejich pomnutí bezodkladně zrušena.

HK ČR si je vědoma nutnosti zajištění kybernetické bezpečnosti a bezpečnosti informací, a to v celé síti, proto v rámci ustanovení § 30 navrhuje nově zavést taktéž povinnost pro poskytovatele strategicky významné služby provést analýzu rizik spojených s dodavatelem dotčeným opatřením obecné povahy u těch aktiv strategicky významné služby, které poskytovatel strategicky významné služby nezařadil do kritické části stanoveného rozsahu dle § 28 odst. 3 písm. a). Jedná se v podstatě o zavedení jakési kaskády bezpečnostních opatření, kdy pro tu nejkritičtější část strategické infrastruktury, kde hrozí přímý okamžitý dopad na nedostupnost strategicky významné služby, bude uvalena povinnost řídit se případným omezením či zákazem uvedeným v opatření obecné povahy, a pro ty méně kritické části strategické infrastruktury bude nově dána povinnost zohlednit rizika identifikovaná státem a implementovat odpovídající bezpečnostní opatření.

Na základě analýzy rizik poskytovatel strategicky významné služby vypracuje plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy, který musí pravidelně (alespoň jednou za kalendářní rok) aktualizovat



Předkladatel tedy bude moci omezit či zakázat plnění dodavatele v kritické části stanoveného rozsahu tam, kde hrozí nedostupnost strategicky významné služby. Pro zbytek aktiv pak vznikne poskytovatelům strategicky významné služby automaticky povinnost provést analýzu rizik uvedených v opatření obecné povahy i pro aktiva nezařazená do kritické části stanoveného rozsahu a vypracovat strategii zvládání rizik včetně implementace odpovídajících bezpečnostních opatření.

HK ČR se domnívá, že takto navržený postup, který vychází z předpokladu účasti vlády na rozhodování (vzhledem k tomu, že se jedná o otázku se zahraničně-politickým přesahem) a konzultacemi se sektorovými regulátory, lze, na rozdíl od postupu stanoveného návrhem ZKB, považovat za proporcionální a vhodný a přiměřený z hlediska dotčených subjektů.

33. Připomínka k § 30

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl za text § 30 vložen nový § 31 takto:

„§ 31

Náhrada účelně vynaložených nákladů

- (1) V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle § 30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 9 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle odstavce 3 a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost.***
- (2) Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení.***
- (3) Zrušením opatření obecné povahy podle odstavce 11 nezaniká právo na náhradu nákladů podle tohoto odstavce. Ve věci náhrady nákladů podle tohoto odstavce jménem státu jedná Úřad.“***

a § 31 až 73 byly přečíslovány na 32 až 74.

Odůvodnění:

HK ČR je přesvědčena, že není možné, aby do procesu omezování dodavatele, což je fakticky velmi zásadní a závažný zásah do svobody podnikatelského prostředí, byl zapojen pouze předkladatel a ostatní státní orgány, především ty s politickou odpovědností, byly zapojené v procesu pouze okrajově poskytováním součinnosti či poskytováním informací.

HK ČR proto navrhuje vložení úpravy náhrady škody, a to podobně, jako je tomu např. v § 16n zákona č. 289/2005 Sb., o vojenském zpravodajství, v němž je přiznána náhrada škody každému, komu škoda nebo nemajetková újma vznikla v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu:

- „(1) Každý, komu vznikla škoda nebo nemajetková újma v souvislosti s činnostmi Vojenského zpravodajství, jimiž se podílí na zajišťování obrany státu, má právo na jejich náhradu.***
- (2) Fyzické nebo právnické osobě se nahrazuje také škoda nebo nemajetková újma, která jí vznikla v důsledku realizace opatření přijatých Vojenským zpravodajstvím v zájmu provedení aktivního zásahu směřujícího k odstranění kybernetického útoku nebo hrozby v rámci zajišťování obrany státu v kybernetickém prostoru.***



- (3) *Povinnost státu k náhradě škody nebo nemajetkové újmy podle odstavců 1 a 2 nevznikne, pokud se jedná o škodu nebo nemajetkovou újmu způsobenou fyzické nebo právnické osobě, která vyvolala útok nebo hrozbu.*
- (4) *Za škodu nebo nemajetkovou újmu způsobenou Vojenským zpravodajstvím odpovídá stát. Náhradu škody nebo nemajetkové újmy poskytuje v zastoupení státu Ministerstvo obrany.*“

Náhrada škody je upravena v nově navrhovaném ustanovení § 31, podle kterého má poskytovatel strategicky významné služby vůči státu nárok na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností z opatření obecné povahy.

Náhrada škody dle předmětného ustanovení je koncipována jako náhrada za nemožnost používání technologie po plnou dobu jejího životního cyklu a konkrétní výše je určována znalcem, a to na základě daňových odpisů, s tím, že by byla určena na základě rozdílu mezi délkou životního cyklu plnění dodavatele a lhůty stanovené předkladatelem pro omezení či odstranění plnění dodavatele. Metoda určení výše náhrady škody dle odpisů se použije právě a jen pro případy náhrady za nemožnost používání dlouhodobého majetku v plném rozsahu. Pokud by tedy např. předkladatel stanovil lhůtu pro odstranění plnění dodavatele v délce 3 roky a životní cyklus plnění dodavatele (technologie) by byl dle daňových odpisů 5 let, mohl by poskytovatel strategicky významné služby požadovat náhradu škody odpovídající 2 zbývajícím rokům odpisů. Pro náhradu dalších účelně vynaložených nákladů vzniklých v důsledku plnění povinností uvedených v opatření obecné povahy se metoda odpisů z povahy věci nevyužije.

Pro zajištění větší právní jistoty státu je maximální doba odpisů omezena na 7/9 let, aby nedocházelo k umělému protahování odpisů, pokud dojde ke změně §28 odst. 3 písm. a). V opačném případě je nutné respektovat životnost zařízení okrajových částí sítě, která je zpravidla násobně delší.

Pokud bude rozsah regulace nastaven tak, jak je uvedeno v tomto návrhu, lze říci, že kompenzace např. v oblasti telekomunikací nebudou žádné. Ustanovení je však nastaveno tak, že pokud by škoda způsobena byla (například v jiných dotčených sektorech), nebo by došlo k novelizaci zákona a rozšíření rozsahu regulace, existovala by zde zákonná možnost nárokovat náhradu škody, což je zásadně žádoucí z hlediska mitigace případných nákladů povinných osob vzniklých v důsledku reflektování opatření obecné povahy.

34. Připomínka k § 31 odst. 4

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byly v § 31 za stávající odst. 4 vložen nový odst. 5 takto:

„(5) Veškeré informace týkající se rozhodnutí o povolení výjimky a řízení o povolení výjimky jsou považovány za neveřejné informace.“

Odůvodnění:

Vzhledem k citlivosti informací, které jsou v rozhodnutí o povolení výjimky uvedeny, je potřebné zajistit, aby rozhodnutí nebylo veřejně dostupné. S ohledem na potřebu zajištění kybernetické bezpečnosti a ochrany informací, jakož i obchodního tajemství dotčených subjektů, není přípustné, aby bylo rozhodnutí o povolení výjimky veřejně dostupné. Zveřejnění informací o tom, komu a za jakých podmínek byla předkladatelem povolena výjimka, je z hlediska cíle zajištění kybernetické bezpečnosti, jakož i z hlediska hospodářské soutěže a ochrany údajů zásadně nevhodné a v rozporu se smyslem zákona.

35. Připomínka k § 32 odst. 1

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby bylo slovní spojení „identifikace všech bezpečnostně významných dodávek“ použité v ustanovení § 32 odst. 1 zpřesněno v tom smyslu, že bezpečnostně významnou dodávkou plynoucí z



rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky), a to ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na poskytovatele strategicky významné služby kladena neúměrně vysoká administrativní zátěž a stejně tak by byl předkladatel zatížen řadou nadbytečných hlášení bez přidané informační hodnoty.

Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění.

Vypořádání připomínky z veřejné konzultace nereflektuje, že návrh se vztahuje k opakovanému objednávání stejného plnění (zboží) tedy nezměněného bezpečnostního rizika.

36. Připomínka k § 32 odst. 2

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text § 32 odst. 2 doplněn tak, že se doba 1 roku ode dne doručení písemného vyrozumění o zápisu se vztahuje i na povinnost zjišťovat informace podle § 32 odst. 1 písm. a), a to ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit předkladateli informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby poskytovatelé strategicky významných služeb zahájili sběr informací bezprostředně po účinnosti zákona, bez stanovení přechodného období.

Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že plnění povinnosti zjišťovat informace nelze zahájit okamžitě. K okamžiku zápisu do evidence poskytovatelů regulované služby nebude mít poskytovatel strategicky významné služby nastaveny odpovídající smluvní a compliance mechanismy a v případě kontroly bezprostředně po tomto zápisu by čelil riziku významných sankcí ze strany předkladatele. I proto je třeba nastavit odložené plnění povinnosti, aby bylo možné zavést příslušné smluvní a compliance mechanismy.

37. Připomínka k § 33

HK ČR pro případ, že nebude akceptována připomínka ohledně zrušení (vypuštění) celého Dílu 5, požaduje, aby byl text v § 33 upraven takto:

„Poskytovatel strategicky významné služby v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek může závazek ze smlouvy na veřejnou zakázku vypovědět bez zbytečného odkladu poté, co zjistí, že v jeho plnění nelze pokračovat, aniž by nebylo porušeno opatření obecné povahy podle § 30.“

Odůvodnění:

I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledán rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek.

Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že některé kontrakty na bezpečnostně významné dodávky jsou dlouhodobé a mohly být sjednány před přijetím navrhované právní úpravy, a tedy ji nemohly předvídat a nemusí v nich být obsažen adekvátní výpovědní důvod.

38. Připomínka k § 34

HK ČR požaduje, aby byl text § 34 upraven takto:

- „(1) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby v ~~rozsahu kritické části stanoveného rozsahu ve stanoveném nezbytném~~ **čas, a kvalitě a rozsahu** z území České republiky.
- „(2) Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupné služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy Vyhlášky o regulovaných službách je povinen zajistit dostupnost jím poskytované strategicky významné služby poskytování veřejně dostupné mobilní služby elektronických komunikací nebo zajišťování veřejné mobilní komunikační sítě elektronických komunikací a nebo poskytování veřejně dostupné služby elektronických komunikací v pevném místě, a to v rozsahu kritické části stanoveného rozsahu a ve stanoveném čase a kvalitě z území České republiky.“
- (23) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby **podle odst. 1 a 2** ~~v rozsahu kritické části stanoveného rozsahu z~~ území České republiky nejméně jednou za dva roky.
- (34) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 ~~a 2 až 3~~ pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2.
- (45) ~~Stanovený~~ **Nezbytný** čas, a-kvalitu **a rozsah** služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu.
- (56) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a).
- (7) Pokud je pro strategicky významnou službu orgánu veřejné správy využíván informační systém veřejné správy^{x)}, pro který je využíván cloud computing, musí být dostupnost takového informačního systému státní správy na území České republiky pro účely zajištění dostupnosti strategicky významné služby dle odst. 1 zajištěna pouze pro informační systémy veřejné správy zařazené do nejvyšší bezpečnostní úrovně.

^{x)} Ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.“

Odůvodnění:

Ustanovení § 34 návrhu zákona stanoví povinnosti na zajištění dostupnosti strategicky významných služeb z území České republiky. Pro veřejnou správu je strategicky významná služba definována jako „výkon svěřených pravomocí“ ze strany vymezených orgánů státní správy a samosprávy. Vymezený okruh orgánů je velmi široký a zahrnuje mimo jiné všechny ústřední orgány státní správy, správní úřady s celostátní působností, kraje, větší obce s rozšířenou působností, vysoké školy, orgány soudní moci a policejní útvary a dalších orgány (dále označovány také jako „orgány veřejné moci“). Dostupnost na území České republiky musí být podle navrhované právní úpravy zajištěna pro všechna aktiva, u kterých by narušení bezpečnosti informací mělo kritický a vysoký dopad na výkon



kterékoli agendy svěřené těmto orgánům. Tato povinnost by se tak v praxi vztahovala na převážnou většinu informačních systémů v české státní správě a samosprávě.

Ačkoliv hlavním cílem nového zákona o kybernetické bezpečnosti má být implementace směrnice NIS 2, požadavek na zajištění dostupnosti služeb z území České republiky nemá ve směrnici žádnou oporu a jde nad rámec její implementace do českého právního řádu. Lze i dovozovat, že tento požadavek může být v rozporu s přeshraniční spoluprací v rámci Evropské unie, kdy elektronizace některých agend veřejné správy probíhá ve vzájemné koordinaci jednotlivých zemí. Zdá se, že se jedná o požadavek, který nebyl v navrhované podobě zatím implementován v žádném jiném členském státě EU.

Z praktického hlediska to znamená, že orgány veřejné moci by musely mít zajištěnou dostupnost veškerých informačních systémů používaných pro výkon svých agend z území České republiky. Pro tyto informační systémy by tak musela existovat záložní varianta, která by byla za všech okolností dostupná výhradně z území České republiky (dle výkladu předkladatele se musí jednat o variantu, která umožní výkon svěřených pravomocí výhradně s využitím aktiv umístěných na území České republiky a nelze ji zajistit např. dvěma zahraničními poskytovateli či privátním připojením).

Tyto požadavky mají zásadní dopad na možnost využívání cloudových služeb v české veřejné správě. Orgány veřejné moci by při využití globálních cloudových služeb musely vytvářet paralelní infrastrukturu na území České republiky (tj. zajistit veškerá aktiva paralelně i na území České republiky, tak aby výkon jejich agend byl možný jen s využitím těchto aktiv). To by vedlo k extrémnímu navýšení nákladů na informační systémy. Tato paralelní infrastruktura by musela být trvale udržována, aktualizována, testována a zabezpečena. Pro některé komplexní SaaS a PaaS služby nemusí být zajištění řešení dostupného výhradně z území České republiky vůbec reálné a tyto služby by tak v české veřejné správě nemohly být vůbec využívány. Tento požadavek by velmi pravděpodobně znemožnil využívání zejména vysoce inovativních služeb s prvky umělé inteligence, které není reálné zajistit výhradně z území České republiky, a to ani s vynaložením vysokých nákladů.

Požadavek na zajištění dostupnosti služeb (z lokálního území) považuje HK ČR za opodstatnitelný pouze pro nejkritičtější infrastrukturu státu.

Pro veřejnou správu byla tato nejkritičtější informační infrastruktura státu již vymezena prostřednictvím bezpečnostních úrovní (bezpečnostní úroveň 4 – kritická) ve smyslu vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (která má být nově vydaná ve stejném znění na základě nově předvídaného zmocnění v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy). Pro tyto systémy je již v souladu s § 6m odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy, možné využívat cloudové služby pouze, pokud jsou poskytovány státním poskytovatelem cloud computingu (tj. je zajištěna dostupnost i poskytování z území České republiky).

Rozšiřování těchto povinností na jakékoliv další systémy veřejné správy tak popírá smysl této úpravy a je nepřiměřené. Dopady takového rozšíření by zahrnovaly několikanásobné navýšení nákladů na informační systémy veřejné správy a výrazné zpomalení rozvoje služeb eGovernmentu a digitalizace státní správy.

Vzhledem k tomu, že oblast elektronických komunikací je velmi specifickým sektorem a již krátce po zveřejnění návrhu ZKB v eKLEP bylo zřejmé, že úprava navržená v návrhu ZKB (ve spojení s příslušnými prováděcími právními předpisy) způsobuje výkladové nejasnosti ohledně rozsahu a dopadu daného ustanovení, navrhuje se zakotvení speciální úpravy zajištění dostupnosti strategicky významné služby pro oblast elektronických komunikací, a to s cílem zamezit možným dezinterpretacím daného ustanovení pro oblast elektronických komunikací, které v případě nezakotvení ustanovení v zákoně hrozí.



Předkladatel na základě připomínek veřejnosti upustil od požadavků na lokalizaci dat na území České republiky nebo spřátelených států. Zároveň však navrhl nahradit lokalizaci povinností zajistit dostupnost strategicky významných služeb z České republiky, pokud jsou k jejich poskytování využívána zahraniční aktiva. Povinnost má zajistit dostupnost nejkritičtějších služeb pro občany České republiky v případě mimořádných událostí (přírodní katastrofy, pandemie, války atp.), které by mohly omezit možnosti využití zahraničních aktiv, ať už z důvodu faktické vzdálenosti, nebo nemožnosti uplatňovat státní moc na území jiných států.

Předkladatel však prostřednictvím strategicky významných služeb spojil mechanismus zajišťování minimální úrovně dostupnosti s mechanismem prověřování bezpečnosti dodavatelského řetězce, přičemž se jedná o odlišné instituty jak z hlediska cíle právní úpravy, tak z hlediska způsobu jeho dosahování.

Účelem stanovení minimální úrovně dostupnosti by mělo být zabezpečení dostupnosti nejkritičtějších služeb na „minimální“ úrovni potřebné k fungování společnosti a státu. Navrhovaná právní úprava se však nezaměřuje na stanovení takové minimální úrovně, kterou částečně ponechává na povinných osobách, nýbrž se věnuje konkrétním funkcím technických aktiv stanoveným ve vyhlášce o nepominutelných funkcích stanoveného rozsahu. Ohledně zabezpečení minimální úrovně dostupnosti tedy ponechává v nejistotě jak poskytovatele, tak uživatele regulovaných služeb.

Z výše uvedených důvodů se navrhuje oddělení mechanismu bezpečnosti dodavatelského řetězce od stanovování minimální úrovně dostupnosti. Minimální úroveň dostupnosti jednotlivých kritických služeb by měla být určena zákonem, přičemž způsob zajištění její dostupnosti by měl být ponechán na poskytovatelích. Zároveň se navrhuje konkrétní výčet služeb pro sektor telekomunikací, která respektuje přiměřenou úroveň služeb elektronických komunikací v souladu se zákonem č. 127/2005 Sb., o elektronických komunikacích.

Poskytovatelé a zajišťovatelé veřejně dostupných služeb elektronických komunikací by měli mít povinnost zajistit dostupnost hlasové komunikace v mobilní síti a připojení k internetu v mobilní síti v takovém rozsahu tak, aby byla při mimořádné situaci umožněna základní komunikace mezi občany a orgány veřejné moci. Minimální úroveň by tak měla zabezpečit komunikaci během mimořádné situace, aniž by kladla nadměrné technické nároky na poskytovatele, přičemž se nepočítá s nutností zajišťovat služby, které vyžadují vysokou rychlost internetového připojení, jako např. streamování videí nebo videohovory.

Pokud by měla být zachována povinnost zabezpečit dostupnost regulované služby v celém rozsahu, k čemuž vede navrhovaná podoba, museli by poskytovatelé služeb elektronických komunikací budovat infrastrukturu výlučně na území České republiky, neboť by nedávalo ekonomický smysl budovat jakoukoli infrastrukturu v zahraničí, pokud by zároveň musela existovat její plnohodnotná „záložní kopie“ v České republice. Taková povinnost by tudíž ani byla nepřípustným omezením volného trhu v rámci EU.

39. Připomínka k § 40 odst. 1

HK ČR požaduje, aby bylo v § 40 odst. 1 vypuštěno písm. g) a stávající písm. h) přečíslováno na g).

Odůvodnění:

Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku, může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken, a to v definovaném rozsahu s odhadnutelným dopadem.



40. Připomínka k § 53 odst. 1

HK ČR požaduje, aby byl text § 53 odst. 1 upraven takto:

„(1) Úřad a provozovatel Národního CERT zpracovávají osobní údaje, jsou-li nezbytné pro výkon jejich působnosti. Tyto údaje Úřad a provozovatel Národního CERT předávají **oprávněným** orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich ~~úkolů~~ **zákonných povinností** a nedojde-li tím k porušení povinnosti mlčenlivosti ~~podle tohoto zákona~~.“

Odůvodnění:

Je nezbytné zajistit soulad s účinnými právními předpisy (jako je např. GDPR), které specifikují pravomoci a zmocnění oprávněných orgánů při plnění jejich zákonných povinností, nejen podle tohoto zákona.

41. Připomínka k § 53 odst. 3 písm. a) až c)

HK ČR požaduje, aby byl obsah § 53 odst. 3 písm. a) až c) uveden do souladu s požadavky GDPR a dalšími předpisy ve smyslu níže uvedeného odůvodnění.

Odůvodnění:

V případě, kdy mají být subjektům údajů odepřena jejich práva, je nutné zákonem vymezit konkrétní účely a podmínky zpracování osobních údajů, a to včetně retenčních povinností. Současně je nutno zakotvit zákonný mechanismus kontroly oprávněnosti a zpracování takovýchto osobních údajů.

42. Připomínka k § 55 odst. 1

V návaznosti na shora uvedené připomínky HK ČR požaduje, aby byl text § 55 odst. 1 upraven takto:

„(1) Prováděcí předpis stanoví

- a) kritéria pro identifikaci regulované služby (§ 4),
- ~~b) způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3),~~
- eb)** bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4),
- ~~ec)~~ **ed)** způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3),
- ~~ed)~~ obsahové náležitosti, formát a způsob oznámení provedení protiopatření a jeho výsledku (§ 20 odst. 3),
- ~~f) kritéria pro identifikaci strategicky významné služby (§ 27 odst. 1),~~
- ~~g) nepominutelné funkce stanoveného rozsahu (§ 28 odst. 4),~~
- ~~h) kritéria rizikovosti dodavatele a způsob jejich vyhodnocení (§ 28 odst. 4),~~
- ~~if)~~ **ig)** způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a
- jg)** technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů uvedených v § 44 odst. 2 (§ 44 odst. 3).“

Odůvodnění:

Navrhovaná úprava obsahu § 55 odst. 1 je důsledkem požadavku HK ČR na zrušení zákonného zmocnění předkladatele k vydání prováděcích právních předpisů k ustanovením, která mají být v zákoně, případně mají být zcela vypuštěna.

43. Připomínka k § 58 odst. 15 písm. a) a písm. b)



HK ČR požaduje upravit text takto:

„(15) *Za přestupek lze uložit pokutu do*

- a) *250 000 000 Kč nebo, tam, kde je to vzhledem k okolnostem přiměřené, do výše 2 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 1 písm. a), písm. d) až k) a písm. m) až p), odstavce 3 písm. a), e) a f), odstavce 6 písm. b) a odstavce 8 písm. a) a b).*
- b) *175 000 000 Kč nebo, tam, kde je to vzhledem k okolnostem přiměřené, do výše 1,4 % čistého celosvětového ročního obratu dosaženého právnickou osobou nebo, pokud je obviněný součástí konsolidačního celku, dosaženého konsolidačním celkem za bezprostředně předcházející účetní období, podle toho, která z daných částek je vyšší, jde-li o přestupek podle odstavce 2 písm. a), písm. d) až k) a písm. m) až p) a odstavce 8 písm. d).“*

Odůvodnění:

Znění návrhu zákona věrně implementuje znění směrnice, která v souladu s judikaturou k soutěžním článkům 101 a 102 SFEU konstatuje možnost uložení pokuty za přestupek vypočítané na základě obratu podniku ve smyslu soutěžního práva, tj. ekonomické jednotky/skupiny, ke které pachatel patří. V souladu s judikaturou SDEU zdůrazňuje HK ČR „pouhou“ možnost takového postupu, tedy zabránění automatickému používání obratu skupiny jako stropu pro výpočet pokuty u pachatele, který náleží do (nějaké) skupiny/konsolidačního celku.

44. Připomínka k § 65 odst. 4

HK ČR požaduje, aby byl text § 65 odst. 4 upraven takto:

„(4) ~~Pokud má být řízení Rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb podle § 11 odst. 2 zahájeno z moci úřední, může být rozhodnutí o výmazu z evidence poskytovatelů regulovaných služeb prvním úkonem v řízení; v takovém případě se rozhodnutí písemně nevyhotovuje, záznamem ve spisu rozhodnutí o výmazu nabývá právní moci a Úřad provede výmaz z evidence poskytovatelů regulovaných služeb.~~“

Odůvodnění:

Ustanovení § 65 odst. 4 si v hypotéze klade za podmínku zahájení řízení podle § 11 odst. 2 z moci úřední. Řízení podle § 11 odst. 2 však nemůže být zahájeno na žádost, tudíž se vždy musí jednat o řízení z moci úřední.

Z tohoto důvodu navrhuje vymazat nadbytečnou podmínku.

45. Připomínka k tezí vyhlášky o regulovaných službách – Kritéria pro identifikaci regulované služby

HK ČR požaduje, aby ve vyhlášce o regulovaných službách v Příloze v bodě 16.1 a 16.2 sjednotit kritéria na 350 000 SIM karet nebo pevných přípojek. Alternativně obě tato kritéria zrušit a ponechat pouze dělení vyplývající ze směrnice.

Odůvodnění:

Česká republika je charakteristická velmi vysokým počtem poskytovatelů přístupu k internetu v pevném místě. Tato skutečnost vede k pozitivním jevům v oblastech hospodářské soutěže a různorodosti použitých řešení. Subjekty působící na trhu přístupu k internetu v pevném místě jsou ale vlivem silného konkurenčního boje a (z podstaty věci) jejich omezené hospodářské síly více

zranitelné vlivy nadměrné regulační zátěže. Stanovení hranice 100.000 přípojek v pevném místě jako kritéria pro identifikaci poskytovatele strategicky významné služby je z tohoto důvodu nevhodné, neboť bez zjevného důvodu vystaví i nižší kategorii (co do rozsahu) poskytovatelů dramatickému nárůstu jejich regulačních povinností – a to i v případě, že záležitosti související s bezpečností svých sítí spravují odpovědně. Umístění dané hranice v předkládaném návrhu je navíc drasticky nesystémové s ohledem na skutečnost, že na trhu mobilním, který je dominován velkými nadnárodními poskytovateli, je hranice nastavena na 3,5 násobek.

Na českém trhu je běžné, že řada operátorů provozuje své sítě jako holding menších společností. Jde o reziduum toho, že některé operátorské skupiny zvláště regionálních hráčů vznikly tak, že provedly akvizice menších hráčů. Protože operátoři mají různé využití technologie, různé dodavatele, různé topologie sítí a různou praxi v nasazování technologií do sítě, má smysl docházet k nějakému sjednocování až v určitém čase, případně – pokud operátorské holdingy seznají, že je to vhodné – k technologické unifikaci nedojít vůbec. Takto vzniklé skupiny mohou překonat předkladatelem stanovený limit 100 tisíc aktivních pevných přípojek, ačkoli se de facto jedná o malé podniky. Vzhledem k této běžné praxi je HK ČR přesvědčena, že by předkladatel měl ustoupit od stanovení objemových kritérií v oblasti pevných sítí, nebo je sjednotit se stanoveným limitem pro mobilní sítě (350 tisíc aktivních přípojek). Dobrou orientací pro tržní poměry na trhu pevného internetu má Český telekomunikační úřad, který vydává přehled o trhu ve svých výročních zprávách <https://www.ctu.cz/vyrocnizpravy>.

Objemový požadavek, pokud by měl být zachován, by měl kvantifikovat nikoliv počet přípojek celkem, ale počet přípojek v rámci jedné infrastruktury.

HK ČR zároveň žádá o upřesnění toho, jak bude předkladatel postupovat v případě operátorů, kteří nabízejí své služby formou tzv. Fixed Wireless Access (FWA) na kmitočtech, které jsou určeny pro služby IMT (3400-3800 MHz). Tito operátoři nabízejí službu, kterou pro některé regulační účely ČTÚ označuje jako pevnou službu, ale zároveň ji nabízí na zařízeních, která mohou mít v sobě SIM kartu a služba je nabízena na kmitočtech harmonizovaných pro pohyblivou službu. Potenciálně mohou mít tyto operátoři časem více než 100 tisíc zákazníků.

46. Připomínka k bodu 1.11 a 1. 14 přílohy – Vyhláška o nepominutelných funkcích stanoveného rozsahu

HK ČR požaduje, aby byl text bodů 1.11 a 1.14 Vyhlášky o nepominutelných funkcích stanoveného rozsahu vypuštěn a ostatní body odpovídajícím způsobem přečíslovány.

Odůvodnění:

Uvedené typy aktiv nepovažuje HK ČR za nezbytné pro zajištění fungování jádra sítě elektronických komunikací, a proto by neměly tvořit součást nepominutelných funkcí stanoveného rozsahu.

47. Připomínka k bodu 11 přílohy – Vyhláška o kritériích rizikovosti dodavatele

HK ČR požaduje, aby byl text bodu 11 Vyhlášky o kritériích rizikovosti dodavatele vypuštěn a ostatní body odpovídajícím způsobem přečíslovány.

Odůvodnění:

Bod 11 přílohy vyhlášky nesměřuje k ochraně vůči dodavatelům, kteří představují bezpečnostní hrozbu pro Českou republiku nebo vnitřní či veřejný pořádek, ale proti dodavatelům, kteří by potenciálně nemuseli být schopni dostát svým smluvním závazkům.

Čistě ekonomické schopnosti dodavatelů jsou záležitostí podnikatelského rizika poskytovatelů strategicky významných služeb, kteří pravděpodobně disponují podrobnějšími informacemi o sektoru, v němž podnikají, než orgány státní správy.



Jedná se tudíž o nadbytečné ustanovení, které má zbytečný potenciál omezovat svobodu podnikání poskytovatelů strategicky významných služeb.

48. Přípomínka k § 10, odst. 1, písm. f) přílohy – Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností

HK ČR požaduje, aby byl text § 10, odst. 1, písm. f) Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností vypuštěn a písm. g) označeno jako písm. f).

Odůvodnění:

Navrhovaná úprava stanovuje svým adresátům povinnost vynucovat určitý obsah smlouvy vůči třetím osobám, s nimiž vstupuje do obchodního styku. Z podstaty věci jsou tyto třetí osoby zahraničními subjekty s často mezinárodním dosahem. Typický adresát úpravy – například poskytovatel služeb elektronických komunikací v pevném místě v České republice – přitom jako zpravidla regionální subjekt menšího rozsahu nemá vyjednávací pozici, která by mu umožňovala vynucovat si libovolné smluvní podmínky vůči jeho dodavatelům. Navrhovaná úprava pro typické adresáty prakticky nesplnitelná. Přijetí navrhované úpravy by mělo potenciálně katastrofické důsledky pro tyto poskytovatele připojení, neboť by hrozilo znepřístupněním prakticky všech dodavatelských vektorů více než 1500 ISP působícím v České republice a omezením hospodářské soutěže na tomto trhu jen na velké nadnárodní společnosti.

C. ZÁSADNÍ PŘIPOMÍNKA K DŮVODOVÉ ZPRÁVĚ

HK požaduje, aby bylo v důvodové zprávě doplněno, zda zjištění rizikovosti dodavatele z hlediska ohrožení bezpečnosti ČR zakládá bezpečnostní událost nebo bezpečnostní incident.

Odůvodnění:

Je třeba najisto stanovit pravidla, podle nichž se bude postupovat.

D. DOPORUČUJÍCÍ PŘIPOMÍNKY

1. Přípomínka k názvu zákona

HK ČR doporučuje v názvu zákona promítnout i slovní spojení „bezpečnost informací“, např. takto: Zákon o kybernetické bezpečnosti a bezpečnosti informací.

Odůvodnění:

Bezpečnost informací je věcnou součástí návrhu, proto by bylo vhodné ji zdůraznit i v názvu zákona.

2. Přípomínka k § 2 odst. 1 písm. g)

HK ČR doporučuje upravit text takto:

„g) řízením kybernetické bezpečnosti **a bezpečnosti informací** činnost poskytovatele regulované služby podle tohoto zákona směřující k zajištění kybernetické bezpečnosti **a bezpečnosti informací** regulované služby.“

Odůvodnění:

Jakkoli je bezpečnost informací součástí kybernetické bezpečnosti, je zcela na místě ji určitým způsobem „vytknout před závorku“, aby byl zdůrazněn její význam, což je ostatně posláním i následující připomínky.

3. Přípomínka k názvu § 13

HK ČR doporučuje upravit název takto:



„§ 13

*Stanovení rozsahu řízení kybernetické bezpečnosti **a bezpečnosti informací** poskytovatelem regulované služby“*

Odůvodnění:

HK ČR má za to, že je nezbytné výslovně stanovit rozsah řízení kybernetické bezpečnosti a bezpečnosti informací.

4. Připomínka k § 45 odst. 1 písm. c)

HK ČR doporučuje upravit text takto:

„c) *dodavatelů bezpečnostně významných dodávek **a dodavatelů s vysokou mírou bezpečnostního rizika,***“

Odůvodnění:

Doporučovaná úprava výrazně napomůže uživatelskému komfortu a bude sloužit k předcházení a eliminaci ve vazbě na případné (a hrozící) bezpečnostní incidenty.

5. Připomínka k důvodové zprávě, § 17 odst. 5

HK ČR doporučuje upravit text důvodové zprávy k § 17 odst. 5 tak, že budou vypuštěna slova „nebo svévolným“ takto:

„*Prvotní hlášení obsahuje informace o tom, zda existuje podezření, že incident byl způsoben nezákonným ~~nebo svévolným~~ zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad.*“

Odůvodnění:

Incident, který vznikl svévolným způsobem, nenaplní podmínky vzniku takového incidentu v kyberprostoru, jak zakládá znění § 16 odst. 1.

6. Připomínka k důvodové zprávě, § 34

HK ČR doporučuje upravit text důvodové zprávy k § 34 takto:

- odst. 1 úplně vypustit;
- text odst. 2 upravit tak, že se za slova „cílů na rizika spojená s dostupností“ doplní slova „poskytované služby“;
- text odst. 2 dále upravit tak, že se za slova „Nicméně je limitován nutností zajistit tuto dostupnost“ doplní slova „řídícím systémem“.

Odůvodnění:

Navrhované znění prvního odstavce důvodové zprávy vychází na původního obsahu § 34 týkajícího se lokalizace a zpracování dat, nicméně změny vyplývající z uplatněných připomínek se zaměřují na zajištění dostupnosti služby výhradně z území ČR. Proto je nedůvodné se nadále zabývat tématem dostupnosti a zpracování dat.

Zároveň je nutné zdůraznit, že dostupnost služby a její obnova znamená realizaci takového opatření, aby v případě obnovy bylo možné takovou obnovu zajistit z území České republiky, a nejedná se o reálné poskytování služby z území České republiky.

HK ČR předpokládá, že předkladatelem bude vytvořen metodický pokyn, který bude upřesňovat a zajišťovat plnění tohoto ustanovení.