Připomínky Výboru nezávislého průmyslu z.s. k návrhu Zákona o kybernetické bezpečnosti.

Obecné připomínky			
1.	Doplnění závěrečné zprávy z hodnocení dopadů regulace - hodnocení dopadů regulace nebylo provedeno dle závazných metodik a je nedostatečné.	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. Metodika obsahuje vzorovou tabulku pro výpočet administrativní zátěže v právním předpise, kterou NÚKIB 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.“ Úřad 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 NÚKIB 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. Dovolujeme 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	**Tato připomínka je zásadní.**

		částka ukazuje, že dopad nového ZKB může být na podnikatelské prostředí extrémně významný a není možné jej v důvodové zprávě nechat nevyčíslený.	
2.	Návrh na doplnění závěrečné zprávy z hodnocení dopadů regulace – doplnění analýzy odůvodnění prověřování dodavatelského řetězce	NÚKIB 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 nijak nerozporujeme. Zcela ale chybí jakýkoli analytický podklad, ze kterého by bylo patrné, z jakých dat úřad 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. NÚKIB přitom v důvodové zprávě tvrdí, že: *Nezřídka 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 mezi část zdůvodnění toho, proč chce stát vůbec mechanismus zavést. Z tohoto textu z Důvodové zprávy vyplývá, že úřad má zjevně z vlastní činnosti k dispozici analýzu reflexe Varování a analýzu reflexe 5G Doporučení mezi povinnými subjekty. Požadujeme, aby Úřad doplnil do důvodové zprávy data z těchto analýz. Dále požadujeme, aby Úřad 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.	**Tato připomínka je zásadní.**

		• Zda zohledňují rizika spojená s dodavatelem, která úřad identifikoval v tezích prováděcího právního předpisu a která zveřejnil v „5G Doporučení“. Jsme přesvědčeni, že bez úplně základní analýzy statu quo není možné přistupovat k jakékoli další regulaci, protože úřad vůbec nemůže mít informace o tom, jak jsou v současnosti tato rizika potenciálními povinnými subjekty vnímána ve světle vydaných opatření a materiálů úřadu, a případně mitigována. Pouze na základě podobné analýzy (a dalších analýz, které zmiňujeme 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.“	
3.	Návrh na doplnění závěrečné zprávy z hodnocení dopadů regulace – vliv na plnění aukčních podmínek	Některé subjekty na trhu elektronických komunikací jsou zároveň držiteli kmitočtových přídělů z aukcí kmitočtů z let 2017 a 2021. Podmínky spojené s přídělem 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. Požadujeme doplnit do důvodové zprávy ve spolupráci s ČTÚ předpokládaný vliv mechanismu na plnění těchto závazků.	**Tato připomínka je zásadní.**

Konkrétní připomínky			
4.	§ 6 odst 3	Požadujeme režim poskytovatele regulované služby stanovit přímo v zákoně (v příloze zákona) z důvodu regulační a právní jistoty. (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.	**Tato připomínka je zásadní.**
5.	§ 10 odst 2	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 regulované služeb v režimu vyšších povinností muset realizovat pomocí zaměstnanců či kontraktorů s konkrétními znalostmi a dovednostmi, které nemusí být v dané organizaci dosud vůbec přítomni. Navíc musí dojít k revizi smluv s dodavateli a k další řadě plnění, které zajistí compliance. U menších poskytovatelů služeb elektronických	**Tato připomínka je zásadní.**

		komunikací může být velká komplikace vůbec nalézt vhodné lidi – pokud předpokládáme 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 úřad bude regulovat nově až 2000 subjektů v odvětví elektronických komunikací, z nichž řada jsou mikropodniky v odlehlých venkovských oblastech. Požadujeme změnit text návrhu takto: *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 vyrozumění o zápisu do evidence poskytovatelů regulovaných služeb až do okamžiku doručení vyrozumění o výmazu z evidence poskytovatelů regulovaných služeb podle § 11.*	
6.	§ 21 odst 1	Směrnice v článku 23 odst 7, ze kterého vychází § 21 „Výstraha“ hovoří pouze o „významných“ incidentech, toto zúžení ale v § 21 chybí, požadujeme jej doplnit. Jinak je oprávnění NÚKIB informovat o kyberbezpečnostních incidentech prakticky bezbřehé. NIS 2 článek 23 odst 7: Pokud je nezbytné informovat veřejnost, aby se významnému incidentu zabránilo nebo aby se probíhající významný incident vyřešil, nebo pokud je zveřejnění významného incidentu jinak ve veřejném zájmu, může tým CSIRT některého členského státu nebo případně jeho příslušný orgán, případně týmy CSIRT nebo příslušné orgány jiných dotčených členských států po konzultaci s dotčeným subjektem informovat veřejnost o významném incidentu nebo požadovat, aby tak učinil daný subjekt. Požadujeme tedy § 21 odst 1 změnit 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.	

7.	§ 22 odst 2	Požadujeme vypustit kompletně celý § 22 odstavec 2. Varování je instrument, který je v ZKB nad rámec směrnice. V původním ZKB je Varování upraveno tak, že jeho obsahem není nic ekvivalentního tomuto odstavci. Jde tedy o typický gold-plating. V důvodové zprávě není nijak zdůvodněno, proč tento odstavec úřad do § 22 vložil. Navíc pokud úřad může „stanovit jinak" jak poskytovatel regulované služby v režimu vyšších povinností Varování zohlední, znamená to významný prostor k širokému zásahu úřadu do svobody podnikání fakticky dle libosti. Úřad 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 tohoto paragrafu tedy neexistuje žádný logický důvod. Požadujeme změnit § 22 takto: § 22 Varování (1) Úřad vydá varování, dozví-li se o závažné kybernetické hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti. ~~(2) Poskytovatel regulované služby v režimu vyšších povinností zohlední varování v rámci stanoveného rozsahu, pokud Úřad nebo jiný právní předpis nestanoví jinak.~~ (2~~3~~) Varování Úřad oznámí dotčeným poskytovatelům regulované služby a zveřejní jej na úřední desce Úřadu. Úřad varování nezveřejní, pokud by jeho zveřejnění mohlo ohrozit zajišťování kybernetické bezpečnosti, účinnost protiopatření vydaného podle tohoto zákona, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat orgán nebo osobu, která kybernetickou hrozbu, zranitelnost nebo s tím související kybernetický bezpečnostní incident ohlásila.	
8.	Díl 5 celkově	Požadujeme vynětí Dílu 5 z NZKB (a odstranění odkazů na ustanovení Dílu 5 v celém zákoně). Alternativně požadujeme minimálně schvalování mechanismu v podobě zvláštního zákonného předpisu mimo implementaci NIS 2. Mechanismus 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-	**Tato připomínka je zásadní.**

		membres-qui-bannissent-huawei-1952702), je tak potřeba pečlivě zvážit (i s ohledem na naše další připomínky), 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. Úřad sám v důvodové zprávě uvádí na straně 69, že kritéria jsou fakticky totožná, jaká navrhuje v mechanismu. Navíc tvrdí, že v podobě § 23 má k dispozici nástroj (reaktivní protiopatření) kterým může povinným osobám nařídit 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 NÚKIB 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 zohlednit výsledky tohoto posouzení, pak je na místě otázka, k čemu je mechanismus na národní úrovni vlastně potřeba.	
9.	Díl 5 celkově	Alternativně, pokud NÚKIB neakceptuje připomínku č. 8, požadujeme: • Pečlivé 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	**Tato připomínka je zásadní.**

		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 NÚKIB 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 NÚKIB Bezpečnostní rada státu ještě před tím, než bylo známé finální znění směrnice NIS 2, zvláště když Úřad sám v důvodové zprávě tvrdí, že v podobě § 23 NZKB má k dispozici nástroj (reaktivní protiopatření) kterým může povinným osobám nařídit zohlednění výsledků koordinovaného posouzení bezpečnostních rizik kritických dodavatelských řetězců. • Koordinované posouzení rizik dodavatelských řetězců na evropské úrovni by dle našeho pohledu 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 valuace jejich společností, což bude mít vliv na případný exit majitelů nebo na získání strategických investorů. NÚKIB by měl tyto aspekty zhodnotit podrobně v analýze RIA, kde zcela absentují. • Upozorňujeme, že existuje „Metodická pomůcka pro prevenci nadbytečné regulatorní zátěže při implementaci práva EU“ dostupná na stránkách Úřadu vlády. Podle kapitoly II „Předcházení nadbytečné regulatorní zátěži při neminimalistické implementaci“ by měl NÚKIB vždy posoudit, zda zvolen varianta implementace nepředstavuje nadbytečnou regulatorní zátěž a posouzení provést při hodnocení dopadů regulace. Požadujeme, aby NÚKIB 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 NZKB. • Případné omezení dodavatelů významně ovlivní investiční kapacitu a schopnosti především menších a středních firem investovat do rozvoje svých sítí. Pokud budou NÚKIB nějací 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.	

		• NÚKIB by měl také zhodnotit vliv na malé a střední podniky v RIA tak, jak to předpokládají příslušná pravidla.	
10.	§ 28 odst 3a)	Úřad 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 našeho přesvědčení 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 jsme přesvědčeni, že identifikace podle prováděcího právního předpisu postačuje k tomu, aby NÚKIB 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. Požadujeme tak zrušit zákonné zmocnění úřadu 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. Úřad 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. Odst 3a) tak požadujeme změnit takto: 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	**Tato připomínka je zásadní.**

		úrovní ~~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,~~	
11.	§ 28 odst 3b)	Úřad zde uvádí, že „pro potřeby mechanismu (…) se rozumí: *b) bezpečnostně významnou dodávkou plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu* *1. technického prostředku nebo vybavení s výpočetní kapacitou,* *2. programového prostředku nebo vybavení, nebo* *3. informační či komunikační služby,* Požadujeme, aby v § 2 byly vymezeny všechny pojmy z tohoto odstavce, především pak bod 3, který není nijak vymezen. „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 předpokládáme, že povinné subjekty by v rámci regulační opatrnosti NÚKIB informovali o všech dodavatelích, kteří se mohou byť 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.	**Tato připomínka je zásadní.**
12.	§28 odst 3c)	Úřad zde uvádí, že *„dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako poddodavatel bezpečnostně významnou dodávku.“* 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 odstavce 3b), což je ale fakticky jakákoli služba, protože NÚKIB 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 NÚKIB dle důvodové zprávy	**Tato připomínka je zásadní.**

		předpokládá, ale na stovky dalších subjektů. Úřad nebere v úvahu fakt, že sektor elektronických komunikací je extrémně propojen řadou dodavatelsko-odběratelských vztahů. Protože mechanismus úřad definuje 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 zohledněný 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“). I z tohoto důvodu požadujeme změnit § 28 odst 3a skutečně jen na kritické části sítě, jak píšeme v připomínce č. 10	
13.	§ 28 odst 4	Úřad by neměl stanovovat „nepominutelné funkce stanoveného rozsahu“ (viz připomínka č. 10). Zároveň by kritéria rizikovosti dodavatele neměly být v prováděcím právním předpise, ale přímo v zákoně (případně v příloze k zákonu). Pokud by byla tato kritéria stanovená pouze úřadem, reálně hrozí, že jakékoli příští vedení úřadu jmenované jakoukoli příští vládou bude mít naprosto odlišný názor na to, jaká mají tato kritéria být a bude je daleko snáze a rychleji moci měnit, což může způsobit zásadní regulační nejistotu. § 28 odst 4 tak požadujeme zcela vymazat. ~~Nepominutelné funkce stanoveného rozsahu a kKritéria rizikovosti dodavatele a způsob jejich vyhodnocení stanoví prováděcí právní předpis.~~	**Tato připomínka je zásadní.**
14.	§28 odst 4 / vyhláška o kritériích rizikovosti dodavatele	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 úřadem 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 úřad a další orgány brát tato technická a organizační opatření v úvahu při rozhodování o rizikovosti dodavatele. Požadujeme tak do kritérií rizikovosti dodavatele doplnit technická a organizační kritéria a výslovně uvést do §4 vyhlášky (nebo do příslušného ustanovení zákona), že technická a organizační kritéria musí být brána v úvahu při vyhodnocování rizikovosti dodavatele a jako mitigační opatření.	
15.	§ 30	Dle našeho přesvědčení není možné, aby do procesu omezování dodavatele, což je fakticky velmi zásadní a závažný zásah do svobody podnikatelského prostředí, byl zapojen pouze NÚKIB 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 rizikovosti dodavatele*“. I kritéria pro hodnocení rizikovosti 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 požadujeme tak 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 kybernetickej bezpečnosti. Podle slovenské právní úpravy Národní bezpečnostní úřad Slovenska	**Tato připomínka je zásadní.**

		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. Námi 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 NÚKIB uvedl v OOP a vypracovat plán zvládání rizik, jehož součástí jsou i bezpečnostní opatření minimalizující rizika spojená s dodavatelem. Navrhujeme tak následující nové znění § 30: § 30 Omezení rizik spojených s dodavatelem 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”). 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 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. 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.	

		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 s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. 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 pominutí 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.	
16.	§ 55, odst. 1	Požadujeme změnu příslušného paragrafu ve světle připomínek výše (zrušení zákonného zmocnění k vydání prováděcích právních předpisů k ustanovením, která mají být v zákoně, případně mají být zcela vypuštěna). Prováděcí právní předpis stanoví a) kritéria pro identifikaci regulované služby (§ 4), ~~b) způsob stanovení režimu poskytovatele regulované služby (§ 6 odst. 3),~~ c) bezpečnostní opatření odpovídající režimu poskytovatele regulované služby a míru a způsob jejich zavedení a provádění (§14 odst. 2 a 4), d) způsob stanovení významného dopadu kybernetického bezpečnostního incidentu na poskytování regulované služby v režimu nižších povinností (§ 16 odst. 3), e) 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),~~ i) způsob hlášení údajů subjektem poskytujícím služby registrace jmen domén (§ 35 odst. 1) a j) technické a organizační podmínky používání Portálu NÚKIB, obsahové náležitosti, formát, strukturu a způsob provádění úkonů uvedených v § 44 odst. 2 (§ 44 odst. 3).“	**Tato připomínka je zásadní.**

K tezím vyhlášek			
17.	Příloha k Vyhlášce o regulovaných službách - Kritéria pro	Požadujeme 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.	**Tato připomínka je zásadní**

	identifikaci regulované služby	Odůvodnění: 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 využité 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 tak operátorské holdingy seznají, že je to vhodné - k technologické unifikaci nedojít vůbec. Takto vzniklé skupiny mohou překonat NÚKIBem stanovený limit 100 tisíc aktivních pevných přípojek, ačkoli de facto jde o malé podniky. Vzhledem k této běžné praxi jsme přesvědčeni, že by NÚKIB měl ustoupit od stanovení objemových kritérií v oblasti pevných sítí, nebo je sjednotit se stanoveným limitem pro mobilní sítě (350 tisíc aktivních přípojek). Dobrou orientaci pro tržní poměry na trhu pevného internetu má Český telekomunikační úřad, který vydává přehled o trhu ve svých výročních zprávách https://www.ctu.cz/vyrocni-zpravy. Objemový požadavek, pokud by měl být zachován, by měl kvantifikovat nikoliv počet přípojek celkem, ale počet přípojek v rámci jedné infrastruktury. Zároveň žádáme o upřesnění toho, jak bude NÚKIB postupovat v případě operátorů, kteří nabízí své služby formou tzv. Fixed Wireless Access (FWA) na kmitočtech, které jsou určené pro služby IMT (3400-3800 MHz). Tito operátoři nabízí službu, kterou pro některé regulatorní účely ČTÚ označuje jako pevnou službu, ale zároveň ji nabízí na zařízeních, které mohou mít v sobě SIM kartu a služba je nabízena na kmitočtech harmonizovaných pro pohyblivou službu. Potenciálně mohou mít tito operátoři časem více než 100 tisíc zákazníků.	

Bc. Jakub Rejzek, MBA, LL.M.
prezident asociace
Výbor nezávislého ICT průmyslu z.s.
jakub.rejzek@vnictp.cz, +420 727938968

Jakub Rejzek

Digitally signed by Jakub Rejzek
Date: 2023.07.18 20:16:02 +02'00'