Formulář k zasílání připomínek k návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů ze strany odborné veřejnosti

Návrh nového zákona o kybernetické bezpečnosti a souvisejících předpisů naleznete ZDE.

NÚKIB upozorňuje, že:

- proces připomínkování návrhu nového zákona o kybernetické bezpečnosti a souvisejících předpisů nenahrazuje meziresortní připomínkové řízení ani žádnou jinou část legislativního procesu, jehož zahájení je plánováno na polovinu roku 2023,
- zveřejněné návrhy nového zákona o kybernetické bezpečnosti a souvisejících předpisů jsou návrhy NÚKIB a lze předpokládat, že budou v souvislosti s připomínkami i následným legislativním procesem měněny (z tohoto důvodu také není nutné připomínkovat formátování, ani další textové úpravy zveřejněných návrhů – na zveřejněné návrhy nejsou v tuto chvíli kladeny plné nároky plynoucí z Legislativních pravidel vlády),
- zasláním připomínky zasilatel potvrzuje, že byl informován o zpracování osobních údajů za účelem vypořádání připomínky, informace o zpracování osobních údajů jsou dostupné ZDE.
- vypořádání připomínky bude zasláno pouze tomu, kdo uvede své kontaktní údaje v příslušné části tohoto formuláře, jinak má Úřad za to, že zasilatel o zaslání vypořádání nemá zájem,
- připomínky budou vypořádávány v co nejkratším termínu, avšak v závislosti na dostupných kapacitách,
- má právo navrhovanou změnu odmítnout (především pokud bude rozporná se zněním směrnice NIS2), případně změnit její navrhovanou podobu při zachování původní myšlenky.

NÚKIB dále upozorňuje, že se bude připomínkami zabývat, pokud splní následující podmínky:

- návrh bude relevantní k dané problematice, bude alespoň stručně zdůvodněn a bude obsahovat základní návrh řešení,
- návrh bude ctít podmínky právního státu a principy, na kterých je postaven zákon o kybernetické bezpečnosti.
- tento formulář s návrhy bude zaslán e-mailem na adresu regulace@nukib.cz s předmětem „**Návrh nového ZKB – připomínka veřejnosti 2023**“, nejpozději do **26. února 2023 včetně**.

Datum:	10.3.2023	Navrhuje (jméno, příjmení, případně organizace):	Svaz průmyslu a dopravy České republiky
Kontaktní údaje pro potřeby konzultace a zaslání vypořádání (e-mail, telefon):			Kateřina Kalužová, kkaluzova@spcr.cz, 721 144 177

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Např.: Zákon o kybernetické bezpečnosti, § X Vymezení pojmů	*Např.: Změnit v definici pojmu (…) slovo (…) na slovo (…)*	*Např.: Původně navrhovaná definice neuvádí důležitý znak tohoto pojmu, a to (…). Navrhovaná změna tento nedostatek odstraní.*	
OBECNÉ ZÁSADNÍ PŘIPOMÍNKY			
Působnost zákona o kybernetické bezpečnosti na poskytovatele usazené v jiném členském státě	Navrhujeme doplnit nové odstavce 4) a 5) s následujícím zněním: „4) Tento zákon se nevztahuje na osoby, které mají sídlo v jiném členském státě, s výjimkou těchto případů: a) poskytovatel veřejně dostupné služby elektronických komunikací *[poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikací];*	Návrh zákona o kybernetické bezpečnosti (dále jen „**návrh zákona**“) v rámci ustanovení *„§ X – Zástupce poskytovatele regulované služby“* implementuje ustanovení článku 26 odstavce 3 a 4 Směrnice (EU) 2022/2555 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2) (dále jen „**směrnice NIS2**“) ohledně povinnosti ustanovit zástupce, v případě, že se povinný subjekt nachází mimo Evropskou Unii. Z předloženého znění se nám však jeví, že návrh zákona neimplementuje odstavce 1 a 2 článku 26 směrnice	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	b) osoba zajišťující veřejnou komunikační síť *[poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikací];* 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 překladu jmen domén (DNS), 2. poskytovatel správy a provozu registru internetových domén nejvyšší úrovně,	NIS2, které určují, jakému právnímu řádu členských států podléhají povinné subjekty a který vyjasňuje, 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). V takovém případě by bylo nezbytné vykládat teritoriální aplikovatelnost zákona prostřednictvím přímé aplikace článku 26 směrnice NIS2, což nepovažujeme za vhodný legislativní postup. V souladu s čl. 26 odstavce 1 a 2 směrnice NIS2 proto považujeme za klíčové vyjasnit na úrovni zákona, že český zákon o kybernetické bezpečnosti se neuplatní na vybrané subjekty, které mají své sídlo či hlavní provozovnu v jiném členském státě či v něm poskytují své služby, a proto podléhají právnímu řádu tohoto členského státu. V souladu s požadavky čl. 26 směrnice NIS2 proto navrhujeme stanovit, že zákon se nevztahuje na poskytovatele usazené v jiném členském státě, ledaže naplňují některou z výjimek stanovených v čl. 26 odst. 1 směrnice NIS2, jak jsou navržené implementovat do nového odstavce 4. Český zákon o kybernetické bezpečnosti se tak uplatní pouze na:	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	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	- 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 NIS2)*; - osoby zajišťující veřejnou komunikační síť v souladu se zákonem o elektronických komunikací na území České republiky *(čl. 26 odst. 1 písm. a) směrnice NIS2);* a ty poskytovatele specifikovaných služeb, kteří mají hlavní provozovnu na území České republiky, navrhujeme implementovat v odst. 4 písm. c) bodech 1 – 10 tohoto návrhu *(čl. 26 odst. 1 písm. b) směrnice NIS2)*.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	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.“		
Lokalizační kritéria Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. Vyhláška o bezpečnostních opatřeních poskytovatele	Navrhujeme <u>zrušit</u> následující ustanovení/předpisy: - Zákon o kybernetické bezpečnosti: *§ X Podmínky lokalizace informací a dat*	Požadavky na lokalizaci dat nevycházejí ze směrnice NIS2, jsou v rozporu s nařízením EU 2018/1807 o rámci pro volný tok neosobních údajů v Evropské unii („**nařízení o volném pohybu dat**“), jakož i harmonizačními záměry EU pro certifikaci služeb cloud computingu (EUCS). Požadavky na lokalizaci dat v České republice také vyjadřují nedůvěru v právní prostředí a	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“	- Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: *Část třetí „Lokalizace informací a dat při zpracování v zahraničí“,* § 29.	ochranu dat v jiných členských státech EU a zcela popírají základní principy evropského trhu a hlavní strategické cíle vytyčené Evropskou unií ve Strategii pro data směřující k jednotnému evropskému datovému trhu. Tyto lokalizační požadavky jsou také v rozporu se Strategií kybernetické bezpečnosti EU, která cílí na společný bezpečný evropský prostor s harmonizovanými pravidly, nikoli na fragmentovaná pravidla vytvářející bariéry pro volný pohyb dat mezi členskými státy. Požadavky na lokalizaci informací a dat nevycházejí z principů směrnice NIS2 a významně přesahují harmonizační rámec a rozsah požadavků, které po členských státech směrnice NIS2 vyžaduje zavést. Směrnice NIS2 je obecně vystavena na principu harmonizace pravidel kybernetické bezpečnosti napříč všemi členskými státy. Česká republika by tak měla tento přístup následovat a nová legislativa kybernetické bezpečnosti by se tak od směrnice NIS2 měla odchylovat jen minimálně. Lokalizační požadavky přitom nejsou standardním bezpečnostním opatřením (resp. bezpečnostním – technickým či organizačním – opatřením), ale jedná se o **významný geopolitický nástroj**, který v dnešním	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		digitálním a globalizovaném může významně determinovat mezinárodní vztahy a fungování jednotlivých trhů (ať už geografických nebo trhu služeb). Cílem předkládané legislativy přitom má být zajištění odpovídající úrovně kybernetické legislativy, nikoliv přijímání zásadních geopolitických a tržních rozhodnutí. Přijetí takto zásadního geopolitického rozhodnutí v oblasti kybernetické bezpečnosti by tak měla být činěna na úrovni EU, nikoliv na území jednoho členského státu – čemuž odpovídá i velmi zásadní debata o přijetí podobných lokalizačních požadavků v rámci připravovaného certifikačního schématu EUCS (Cloud Services Scheme). Implementace lokalizačních kritérií na úrovni jednoho členského státu (České republiky) může mít významné dopady do mezinárodních vztahů se třetími zeměmi (včetně spojenců v NATO a dalších mezinárodních organizacích), ale stejně tak i na vztahy v rámci EU, včetně dopadů na volný trh v rámci EU. Požadavky na lokalizaci údajů představují zjevnou překážku volnému poskytování služeb na vnitřním trhu EU. Neopodstatněné stanovení požadavků na lokalizaci	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		dat je tak v přímém rozporu s požadavky na volný pohyb služeb v rámci EU, stejně jako s přímými požadavky na volný pohyb dat, jak předvídá nařízení o volném pohybu dat. Podle tohoto nařízení o volném pohybu dat jsou veškeré požadavky na lokalizaci dat zakázány, ledaže jsou řádně odůvodněny veřejnou bezpečností. Lokalizační kritéria tak lze stanovovat pouze, pokud takový požadavek lze zhojit významným zájmem na veřejné bezpečnosti České republiky. To však předložená úprava nečiní. Naopak navrhovaná úprava předvídá velmi široce definovaná kritéria, na základě kterých se může požadavek lokalizace dat v České republice vztahovat na většinu informačních systémů, včetně systémů, které nijak nesouvisí s bezpečnostními zájmy České republiky. Požadavek dopadu na bezpečnostní zájmy České republiky není v těchto kritériích nijak zohledněn. Jakékoliv stanovení lokalizačních požadavků (za přijetí premisy, že Česká republika povede svou zahraniční politiku tímto směrem) tak může být odůvodněno jen pro nejzásadnější a nejkritičtější data (resp. systémy s těmito daty nakládající), jako jsou tedy prvky kritické infrastruktury.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		V každém případě platí, že jakákoliv zvažovaná regulace lokalizačních požadavků bude vyžadovat **notifikaci Evropské komisi** v souladu s čl. 4 odst. 2 nařízení 2018/1807, a to včetně řádného zdůvodnění těchto požadavků. Předvídanou úpravou lokalizačních požadavků, jejichž kritéria se v zásadě překrývají s kvalifikačními kritérii bezpečnostní úrovně cloudových služeb veřejné správy „3. Vysoká“ (§ 29 odst. 4 navrhované vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) či „4. Kritická“ (§ 29 odst. 2 navrhované vyhlášky), dochází k vytváření paralelní a protichůdné právní úpravy. Pokud by došlo k přijetí navrhované úpravy, může nastat situace, kdy cloudová služba bude zaregistrovaná v katalogu cloud computingu podle pravidel zákona o informačních systémech veřejné správy, avšak orgán veřejné správy nebude – navzdory zákonné registraci – oprávněn takovou službu využívat, jelikož nebude splňovat lokalizační požadavky podle navrhované úpravy. Předvídaným lokalizačním požadavkům nepomáhá ani přechodná tříletá doba k zajištění souladu s těmito požadavky – zajištění souladu s těmito požadavky bude pro řadu dotčených osob fakticky/technicky	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		nedosažitelné a ve výsledku tyto požadavky povedou k omezení trhu (zejména cloudových služeb), uzavření českého trhu a ve svém důsledku ke snížení úrovně kybernetické bezpečnosti. Povede to také ke snížení dostupnosti nových technologií v České republice a tím pádem i ke snížení konkurenceschopnosti české ekonomiky a vytvoření nežádoucích překážek volnému trhu v rámci Evropské unie. **Z těchto důvodů navrhujeme požadavky na lokalizaci informací a dat z návrhu zákona, včetně souvisejících ustanovení z Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, zcela vypustit.**	
ZKB a současně návrh vyhlášky o Portálu NÚKIB	Holdingové řízení, možnost outsourcingu některých povinností poskytovatele regulované služby	Aktuální návrh nového ZKB (včetně relevantní důvodové zprávy) neobsahuje možnost holdingového řízení, resp. možnost outsourcingu některých povinností poskytovatele regulovaných služeb, byť v minulosti byla tato možnost s NÚKIB diskutována. Pro právě uvedené a s ohledem zejména na malé společnosti nedisponující dostatečným personálním a odborným obsazením a dostatečnými finančními prostředky, navrhujeme výslovně v návrhu nového ZKB zakotvit možnost outsourcingu zákonných povinností	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		jak v režimu vyšších, tak nižších povinností. Níže uvádíme návrh formulace k doplnění: a) *„Plnění povinností poskytovatele regulované služby může být zajištěno i prostřednictvím externích dodavatelů, včetně možnosti zajištění prostřednictvím centralizovaného řešení v rámci podnikatelských seskupení.“* b) V rámci vyhlášky o Portálu NÚKIB navrhujeme výslovnou úpravu právní i technické možnosti vykonávat funkci pověřené osoby pro více poskytovatelů regulované služby (viz praktické využití v rámci centralizovaných řešení větších podnikatelských seskupení).	
Vyhláška o portálu NÚKIB	Specifikovat požadavky	Je důvodné očekávat, že v portále budou povinné subjekty shromažďovat velké množství důvěrných a citlivých informací včetně obchodních tajemství a osobních údajů. S ohledem na rozsah, charakter a citlivost informací shromažďovaných prostřednictvím tohoto portálu by bylo vhodné specifikovat požadavky na úroveň zabezpečení informačních systémů určených pro zpracování těchto informací. Stejně tak by bylo vhodné stanovit informační povinnost Úřadu vůči povinným subjektům v případech, kdy dojde k bezpečnostnímu incidentu,	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		který bude mít za důsledek kompromitaci zpracovávaných informací.	
Vyhláška o portálu NÚKIB	Možné duplicity reportingu poskytovatelů cloudových služeb	§ 1 - Přístup do Portálu NÚKIB a úkony v něm Zde je hlavně hlášení registračních údajů, hlášení kyber incidentů, protiopatření, nápravná opatření… (to není v rozsahu ZoISVS). Dále § 3 Druhy hlášených údajů zde je b) seznam poskytovaných regulovaných služeb naplňujících kritéria pro identifikaci regulovaných služeb Obáváme se, že větší firmy které budou mít zapsané desítky až 100-200 služeb v ISCC (dle ZoISVS), by měly to stejné zapisovat a udržovat v portálu NÚKIB. Pak je v § 3 ještě bod 3): Doplňujícími údaji se rozumí jména domén, čísla autonomních systémů (ASN) a rozsahy IP adres, které jsou využívány k poskytování regulované služby, pokud takové existují, informace o geografickém rozšíření regulované služby, jejím přeshraničním poskytování a vlastnické struktuře poskytovatele regulované služby.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Vypadá to v zásadě duplicitní s údaji, které se mají deklarovat v procesu registrace cloudových služeb dle ZoISVS. Pak § 5 - Změna registrace poskytovatele regulované služby … bod 1) … pokud a) poskytovatel regulované služby naplní kritéria pro identifikaci jakékoliv další regulované služby Rozumíme tomu tak, že to je v zásadě povinnost udržovat seznam regulovaných služeb jako aktuální. Bylo by možné objasnit vztah mezi oběma systémy reportingu? Případně, jestli bude možné údaje využít vzájemně, aby nedošlo ke zbytečné administrativní zátěži?	
ZKB	§ Náležitosti hlášení kybernetických bezpečnostních incidentů	Z povahy věci je většina kybernetických incidentů způsobena nezákonným nebo svévolným zásahem. Není nám tedy jasné, zda povinnost uvádět, zda se domníváme, že incident byl způsobem nezákonným nebo svévolným zásahem, nebude nadbytečná a nebude vést k tomu, že povinné subjekty budou takto hlásit radši každý incident a Úřad tak bude přehlcen falešné „rizikovými“ hlášeními.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Zároveň nám není jasné, jak hodnotit možný přeshraniční dopad incidentu. Obdobně jako výše zastáváme názor, že většina kybernetických incidentů může mít přeshraniční dopad, resp. v oblasti kybernetické bezpečnosti hranice nehrají roli.	
Prověřování bezpečnosti dodavatelského řetězce - Zákon o kybernetické bezpečnosti, Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“ - Vyhláška o nepominutelných funkcích stanoveného rozsahu Vyhláška o kritériích rizikovosti dodavatele	Navrhujeme zrušit následující ustanovení/předpisy: - Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“ zákona o kybernetické bezpečnosti; - Vyhlášku o nepominutelných funkcích stanoveného rozsahu; a - Vyhlášku o kritériích rizikovosti dodavatele. Alternativně, pokud nedojde ke zrušení výše uvedených ustanovení, navrhujeme odstranit z § X Prověřování rizik spojených s dodavatelem, odstavce 3, písm. c)	Požadavky na prověřování bezpečnosti dodavatelského řetězce v současné podobě návrhu zákona opět přesahují požadavky směrnice NIS2. Návrh zákona by se však v této fázi měl zaměřovat především výlučně na implementaci směrnice NIS2, od níž by se měl v co nejmenší míře odchylovat. Komplexnost mechanismu, který zajistí účelnou ochranu subjektů a státu a nutnost jeho vydefinování a precizace se sektorem, kterého se bude týkat, vyžaduje na přípravu více času. Stanovení jasně definovaných podmínek, za kterých může dojít k omezení subjektu v dodavatelském řetězci, ale i forma a rozsah takového omezení nutně podléhá konsenzu státu a subjektů, na kterých připravovaná omezení v budoucnu dopadnou. Je nutné v tomto ohledu stanovit jasné kompetence a pravomoci orgánů státní správy, důslednou reflexi soukromoprávních smluvních vztahů včetně přezkoumatelnosti rozhodnutí, na základě, kterému k jejich omezení může dojít a v neposlední řadě i	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	zákona o kybernetické bezpečnosti, slova *„či jako poddodavatel“*.	možného uplatnění náhrady škody a finančním podílení se státu na mitigaci dopadů takové regulace. Rozumíme, že stanovení požadavků na prověřování bezpečnosti dodavatelského řetězce bylo uloženo NÚKIB Bezpečnostní radou státu na základě jejího usnesení ze dne 21. června 2022 č. 41 k Bezpečnosti dodavatelských řetězců strategické infrastruktury státu, ale takové požadavky by měly být vyčleněny do samostatného právního předpisu. Spojení takto zásadního tématu s implementací směrnice NIS2 může ohrozit implementaci směrnice NIS2 do českého právního řádu v požadované lhůtě. Je tedy vhodné zvážit oddělení celého mechanismu, který není do ZKB implementován na základě NIS 2, od nového návrhu zákona tak, aby nedošlo k dotčení implementační lhůty směrnice NIS 2 a procesu schválení nového ZKB a zároveň aby došlo ke stanovení funkčního procesu pro zvýšení kybernetické bezpečnosti spočívající v omezení dodavatelského řetězce. Za problematické v tomto ohledu považujeme zejména to, že podmínky pro využívání dodavatelů či zákaz využívání (skupiny) dodavatelů stanovuje sám NÚKIB bez konzultace s dalšími (vládními či zákonodárnými)	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		reprezentanty ČR. Stanovením podmínek využívání dodavatelů tak může teoreticky NÚKIB učinit rozhodnutí, které jsou svou povahou především geopolitické a mohou mít zásadní vliv na postavení ČR a její zahraniční politiku. Primárně tak navrhujeme z návrhu zákona zcela vypustit Část „MECHANISMUS PROVĚŘOVÁNÍ BEZPEČNOSTI DODAVATELSKÉHO ŘETĚZCE“ a s tím související prováděcí předpisy – tj. Vyhlášku o nepominutelných funkcích stanoveného rozsahu a Vyhlášku o kritériích rizikovosti dodavatele. V případě, že se NÚKIB rozhodne tuto úpravu ponechat, navrhujeme alespoň upřesnit, že mechanismus prověřování dodavatelského řetězce se týká pouze přímých dodavatelů povinných osob, a nikoliv i dalších nepřímých poddodavatelů. Omezením povinností s prověřováním dodavatelů pouze na úroveň přímých dodavatelů se totiž značně zúží počet subjektů, na něž bude dopadat předmětná úprava a předejde se tak dále situaci, kdy např. povinnosti z předmětné úpravy budou muset plnit také dodavatelé poddodavatelů apod.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB	Poskytovatel regulované služby v režimu nižších povinností	Rozsah bezpečnostních opatření je v režimu nižším i vyšším téměř totožný – na poskytovatele regulované služby v režimu nižších povinností je kladena neúměrná povinnost oproti poskytovateli regulované služby v režimu vyšších povinností. Pokud by tento rozsah zůstal, pak nedává smysl, aby poskytovatel regulované služby v režimu nižších povinností neprováděl řízení rizik, na základě kterého jsou následně stanovena adekvátní opatření. Současně je s režimem nižších povinností spjat institut inspektorů, jakožto subjektů kontrolujících poskytovatele regulovaných služeb v režimu nižších povinností na místo NÚKIB. Náklady na tuto kontrolu si tito poskytovatelé regulovaných služeb nesou ve smyslu návrhu nového ZKB sami (oproti poskytovatelům regulované služby v režimu vyšších povinností) a zároveň de facto podléhají dvoustupňové kontrole, když návrh nového ZKB předpokládá, že protokoly vydané inspektory po kontrole poskytovatele regulované služby v režimu nižších povinností následně překontroluje NÚKIB (opět je zde přísnější režim než v případě poskytovatele regulované služby v režimu vyšších povinností, které kontroluje jen NÚKIB, bez dalšího následného ověření). Ze zkušenosti lze očekávat, že vzhledem k množství povinných subjektů,	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		frekvenci kontrol a rozsahu povinností, dojde k absolutnímu zahlcení úřadu. Každé zjištění z kontrol bude řešeno formou správního řízení. Lze očekávat stovky až tisíce zahájených správních řízení každý rok. <u>Návrhy ke zvážení:</u> a) Umožnění dobrovolného přechodu z režimu nižších povinností do režimu vyšších povinností. - Aktuální návrh české právní úpravy tento přechod neupravuje, nicméně v odůvodněných případech zejména holdingového řízení apod. je umožnění přechodu z režimu nižších povinností do režimu vyšších povinností vhodné pro zajištění jednotnosti procesů a kybernetické bezpečnosti v rámci dotčeného propojeného podnikatelského seskupení. Zároveň tento přechod snižuje administrativní náročnost komunikace, dohledu a kontroly tohoto podnikatelského seskupení ze strany NÚKIB. b) Na příkladu JE – existuje mnoho činností, které budou regulované, ale nejsou předmětem podnikání daného subjektu (core business). U výroby elektrické energie jsou takovými činnostmi např.: - Drážní doprava - Zpracování chemických látek	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		- Provoz skladovacího zařízení (ropa, plyn, vodík) - Provozování vodovodu a kanalizace - Odpadové hospodářství Znamená to, že všechny tyto činnosti budou muset být za danou společnost registrované a budou v rozsahu ISMS? c) Rozlišuje se u výkonu regulované činnosti poskytování služby pouze pro vlastní účely (případně v rámci koncernu) a pro komerční využití? Příkladem v ČEZ je provoz korporátního datového centra. d) Do určovací vyhlášky doporučujeme doplnit větší detail pro snazší „sebeurčení“ – např. některé pasáže z důvodové zprávy nebo odkazy na příslušnou legislativu. Pokud nebude doplněno do vyhlášky, je potřeba vydat detailní metodiku, která doplní Vyhlášku o regulovaných službách, kde budou uvedena zejména jasná kritéria a vodítka – příslušné licence, povolení, zákony apod. (Příklad z odůvodnění vyhlášky: Provozovatel vodovodu je tím, kdo poskytuje řešenou službu, protože jak plyne z § 2 odst. 5 zákona o vodovodech a kanalizacích, je tím kdo „provozuje vodovod a je držitelem povolení k provozování tohoto vodovodu nebo kanalizace vydaného krajským úřadem	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		podle § 6 (tohoto zákona)“. Kritérii, které musí naplnit, aby se stal poskytovatelem regulované služby podle návrhu této vyhlášky pak jsou střední nebo velká velikost daného potenciálního poskytovatele regulované služby.)	
ZKB, návrh vyhlášky o inspektorech	Institut inspektorů	Navrhujeme upustit od záměru vzniku institutu inspektorů. Jedná se o zcela nový institut v oblasti IKB bez existence vhodné analogie, která by fungovala obdobně (zejména aby inspektor nebyl zaměstnancem úřadu a byl jich tak velký počet). Pro pravidelnou kontrolu ze strany inspektora není ani reálný důvod. Na společnost působí desítky jiných zákonů a vyhlášek a jejich dodržování se také pravidelně nepřezkoumává. Pouze v případě nějakého sporu nebo incidentu musí společnost prokázat, že daný zákon/vyhlášku dodržela. Stejný princip je vhodné aplikovat i zde. V případě bezpečnostního incidentu musí být daná společnost schopna prokázat, že měla systém nastavený dle požadavků vyhlášky. Pokud tak neučiní přijde sankce. Je to riziko společnosti, jak se k tomu postaví. <u>Návrhy ke zvážení:</u> a) Změny kontroly inspektorem z aktuálně povinné na dobrovolnou, včetně odstranění povinnosti pravidelných kontrol inspektorem.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Argumentem pro navrhované řešení je snížení personální náročnosti pro obsazení role inspektorů, finanční a administrativní náročnosti pro poskytovatele regulované služby v režimu nižších povinností. Zároveň snížení administrativní, a tedy i finanční náročnosti na straně NÚKIB – zejména snížení počtu správních řízení.	
Návrhy všech dotčených právních předpisů implementujících směrnici NIS2 do českého právního řádu	Zásadní části vyhlášek včlenit do návrhu nového ZKB	Doporučuje důsledně aplikovat zásadu zákonnosti jako stěžejního právního pilíře demokratického právního státu založeného na panství práva. Viz judikatura Ústavního soudu (např. Pl. ÚS 5/93 Povinnosti lze stanovit jen zákonem (35/1994 Sb.) a mnohé další): *„Podle čl. 4 odst. 1 Listiny základních práv a svobod mohou být povinnosti ukládány toliko na základě zákona a v jeho mezích; rovněž podle čl. 2 odst. 4 Ústavy České republiky a čl. 2 odst. 3 Listiny základních práv a svobod nesmí být nikdo nucen činit, co zákon neukládá. Z těchto ustanovení nutno pro oblast působnosti obce dovodit závěr, že v případech, kdy obec vystupuje jako subjekt určující pro občana povinnosti jednostrannými příkazy a zákazy, platí ustanovení čl. 2 odst. 4 Ústavy české republiky a čl. 2 odst. 3 Listiny základních práv a svobod. Obec tudíž může vydávat obecně závazné vyhlášky, jejichž obsahem jsou právní povinnosti, jen na základě a v*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		mezích zákona. K vydání obecně závazné vyhlášky, jejímž obsahem jsou právní povinnosti, je obec proto oprávněna jenom v případě výslovného zákonného zmocnění.“	
ZKB	Různé možnosti uveřejňování informací	Kombinace uveřejňování informací na úřední desce, webových stránkách a Portálů NÚKIB může působit velice nepřehledně. Nejen princip tvorby práva EU „*better regulation*“ vyžaduje pro tvorbu nových povinností zatěžujících adresáty příslušné normy jasná a srozumitelná pravidla. V tomto ohledu by i v případě implementace směrnice NIS2 mělo existovat jedno kontaktní místo - *„single point of contact“*, které bude sloužit k informování všech adresátů nového ZKB o jejich právech a zejména povinnostech.	
ZKB a související vyhlášky	Definování pojmů používaných v návrhu zákona a vyhlášek	Návrhy zákona a vyhlášek transponujících směrnici NIS2 do českého právního řádu pracují často s pojmy, které nejsou definovány v rámci těchto právních předpisů. Jako příklad lze uvést pojmy: uživatel, zákazník (případně zda se jedná o synonymum či dvě různé role), vhodné případy (ve smyslu informační povinnosti poskytovatele regulované služby), uložení na bezpečné místo (ve smyslu Vyhlášky o	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) atd.	
Možný nesoulad návrhu nového ZKB s článkem 26 směrnice NIS2	Návrh na implementaci mechanismu one stop shop	Článek 26 směrnice NIS 2 obsahuje zvláštní pravidla týkající se příslušnosti a teritoriality. Ve vztahu k poskytovatelům služeb DNS, registrům názvů TLD, 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") zavádí směrnice NIS 2 mechanismus jednoho správního místa, podle něhož poskytovatelé spadají do jurisdikce členského státu, v němž mají hlavní provozovnu v Evropské unii (čl. 26 odst. 1 písm. b) směrnice NIS 2). Toto pravidlo je třeba vykládat tak, že poskytovatelé podléhají výlučně právním předpisům pouze jednoho členského státu a řídí se jimi, i když poskytují služby v jiných členských státech. Současně čl. 26 odst. 5 směrnice NIS 2 stanoví povinnosti vzájemné pomoci	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		mezi orgány dohledu s pravomocí nad poskytovateli a orgány dohledu v jiných členských státech. Návrh zákona neprovádí mechanismus jednoho správního místa, jak je stanoven v článku 26 Směrnice NIS2. Zejména: - Čl. 26 odst. 5 směrnice NIS 2 se navrhuje implementovat v části "Vzájemná spolupráce s členskými státy Evropské unie" v kapitole V týkající se pravomocí státní správy, podle které má Národní úřad pro kybernetickou a informační bezpečnost omezené dozorové pravomoci nad poskytovateli, kteří mají hlavní provozovnu v jiných členských státech než v České republice (dále jen "poskytovatelé z jiných členských států"). To potvrzují i důvodové zprávy k návrhu k části "Vzájemná spolupráce s členskými státy Evropské unie". - Čl. 26 odst. 1 písm. b) směrnice NIS 2 se však v Návrhu nenavrhuje implementovat. Naopak podle důvodových zpráv k oddílu "Kritéria regulované služby" v kapitole II týkající se poskytovatelů regulovaných služeb se Návrh vztahuje na všechny poskytovatele regulovaných služeb usazené v České republice nebo poskytující služby	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		České republice, včetně poskytovatelů z jiných členských států. V důsledku této neúplné implementace mechanismu jednoho správního místa podle článku 26 směrnice NIS 2 může být návrh v rozporu se zamýšleným účelem směrnice NIS 2.	
RIA	Upřesnění o konkrétní (zejména finanční a personální) dopady	Vzhledem k rozsahu nové regulace považujeme za vhodné, aby bylo doplněno.	
Konkrétní zásadní připomínky			
LOKALIZAČNÍ POŽADAVKY OBECNĚ		V případě, že by NÚKIB, navzdory rozporu se základními právními principy a předpisy a navzdory výše uvedeným obecným zásadním připomínkám podaným považoval inkorporaci lokalizačních požadavků za odůvodněné z důvodu veřejné bezpečnosti, jsme toho názoru, že **navrhovaná právní úprava obsahuje řadu nedostatků, které činí tyto lokalizační požadavky nesplnitelnými. Jedná se zejména o body, které jsou jednotlivě adresovány v jednotlivých bodech 1 – 8 níže a pro které navrhujeme konkrétní úpravy, jejichž cílem je tyto hlavní nedostatky alespoň částečně mitigovat.**	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
1. ÚZEMÍ PRO LOKALIZAČNÍ POŽADAVKY - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	Navrhujeme omezit lokalizační kritéria pro uchovávání informací a dat na území České republiky (v současnosti upraven jako § 29 odst. 2 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) pouze na nezbytná kritéria, která mohou být ospravedlněna důvody veřejné bezpečnosti. Jiné lokalizační požadavky navrhujeme odstranit.	Požadavky na lokalizaci dat obsažené v navrhované právní úpravě jsou obecně v rozporu s nařízením EU 2018/1807 o rámci pro volný tok neosobních údajů v Evropské unii („**nařízení o volném pohybu dat**“). Podle čl. 4 odst. 1 nařízení o volném pohybu dat jsou veškeré požadavky na lokalizaci dat *„zakázány, ledaže jsou odůvodněny veřejnou bezpečností v souladu se zásadou proporcionality“.* Lokalizační kritéria tak lze stanovovat pouze, pokud takový požadavek lze zhojit významným zájmem na veřejné bezpečnosti České republiky. Kritéria pro lokalizační požadavky pro ukládání dat na území České republiky se v zásadě překrývají s kvalifikačními kritérii bezpečnostní úrovně cloudových služeb veřejné správy „4. Kritická“. **Domníváme se, že lokalizační požadavky pro uchovávání dat na území České republiky by měly být omezeny pouze pro nejkritičtější systémy státu, pro které by byly odůvodnitelné a zhojitelné významným zájmem na zajištění veřejné bezpečnosti**. I taková data by však měla být dovolena uchovávat **kdekoliv na území Evropské unie**, jelikož v opačném případě český zákonodárce předjímá, že ostatní členské státy EU	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		neposkytují dostatečnou úroveň ochrany dat, což se domníváme, není přijatelné. **Tyto požadavky by zároveň měly být omezeny pouze na orgány veřejné správy, které se podílí na zajištění veřejné bezpečnosti České republiky**. To by bylo v souladu s požadavky katalogu cloud computingu, resp. konkrétně s požadavkem ID 1.8 přílohy 2 cloudové vyhlášky. **Lokalizační požadavky stanovené v § 29 odst. 4 vyhlášky na uchovávání dat na území členských států EU, ESVO, NATO nebo OECD jsou rovněž v rozporu s nařízením o volném pohybu dat a s principem volného pohybu služeb v Evropské unii**. Stanovením lokalizačního požadavku dojde k vytvoření neodůvodněné překážky (nezhojitelné odkazem na veřejnou bezpečnost) vstupu zahraničních (včetně tedy evropských) poskytovatelů informačních systémů na český trh, ačkoliv tito poskytovatelé mohou své služby poskytovat standardně v jiných členských státech. Přitom, jak uvádí recitál 7 nařízení o volném pohybu dat, *„za účelem odstranění překážek pro obchod a narušení hospodářské soutěže v důsledku rozdílů mezi vnitrostátními právními předpisy a zabránění vzniku dalších pravděpodobných překážek pro obchod a*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		výrazných narušení hospodářské soutěže, je nezbytné přijmout jednotná pravidla, která se použijí ve všech členských státech". **Česká republika by tak neměla klást speciální požadavky na lokalizaci dat, které nejsou řádně odůvodněné, a to ani tehdy, pokud se lokalizační požadavky týkají uchovávání dat na území členských států EU, ESVO, NATO nebo OECD.** Jakékoliv přijetí těchto požadavků by rovněž podléhalo notifikačnímu řízení vůči Komisi ve smyslu čl. 4 odst. 2 nařízení o volném toku dat. **V rámci této připomínky proto navrhujeme rovněž úplné vypuštění lokalizačního požadavku na uchovávání dat na území členských států EU, ESVO, NATO nebo OECD.**	
2. ZAKOTVENÍ LOKALIZAČNÍCH KRITÉRIÍ NA ÚROVNI ZÁKONA - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat, - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu	Navrhujeme: - zakotvit lokalizační kritéria na úrovni zákona o kybernetické bezpečnosti (např. tedy jako nové odstavce 3 až 6 ustanovení *„§ X Podmínky lokalizace informací a dat"*);	Lokalizační kritéria upravená v návrhu představené v části třetí (§ 29) vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností by měla být podrobena zásadní revizi založené na předvídatelné demokratické diskuzi. Takto zásadní geopolitická rozhodnutí o tom, kde mohou být ukládaná data a za jakých podmínek, by měla být činěna v rámci transparentní parlamentní	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“, - Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy: Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computingu, do bezpečnostní úrovně“.	- zrušit zmocňovací ustanovení k přijetí lokalizačních kritérií (tedy zrušit odstavec 3 ustanovení *„§ X Podmínky lokalizace informací a dat“* zákona o kybernetické bezpečnosti, který umožňuje vymezení konkrétních lokalizačních kritérií).	diskuze, nikoliv na úrovni prováděcích předpisů, které mohou být navíc (na rozdíl od zákonné úpravy podléhající komplexnímu legislativnímu procesu) v zásadě kdykoliv změněny. **Proto navrhujeme, aby jakákoliv úprava lokalizačních kritérií (pokud bude přistoupeno na to, že jsou legitimním nástrojem mezinárodní politiky České republiky) byla zakotvena na úrovni zákona o kybernetické bezpečnosti** – např. tedy jako nové odstavce 3 až 6 ustanovení *„§ X Podmínky lokalizace informací a dat“.* Takto zásadní požadavky nemohou být zakotveny pouze na úrovni prováděcího předpisu (vyhlášky). Doporučujeme proto aplikovat důsledně zásadu panství práva (srov. např. nález např. Pl. ÚS 5/93, podle kterého lze povinnosti lze stanovit jen zákonem) a tyto zásadní požadavky inkorporovat na úrovni zákona. To se týká všech níže uvedených připomínek – pokud tedy budou lokalizační požadavky i přes jejich nesoulad s právem EU přijaty, úprava v § 29 vyhlášky by měla být kompletně zrušena a veškeré požadavky přesunuty do zákona o kybernetické bezpečnosti.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
3. OMEZENÍ ROZSAHU APLIKACE LOKALIZAČNÍCH POŽADAVKŮ NA UCHOVÁVÁNÍ NEAKTIVNÍCH ÚDAJŮ - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - § 29 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	Navrhujeme stanovit, že požadavky na lokalizaci se neuplatní na jakoukoliv *zpracovatelskou* operaci, ale pouze na jejich **uchovávání neaktivních dat**.	Ačkoliv návrh ZKB ani prováděcí vyhlášky neuvádí definici pojmu „zpracování“, lze předpokládat, že se analogicky uplatní definice tohoto pojmu podle Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („**GDPR**“), podle které se jedná v zásadě o jakoukoliv operaci s daty, včetně např. jejich přizpůsobení, pozměnění, vyhledání, nahlédnutí nebo použití. Definice zpracování podle GDPR byla obdobně převzata do vyhlášky č. 316/2021 Sb. o některých požadavcích pro zápis do katalogu cloud computingu (dále jen „**cloudová vyhláška**“). Povinnost zajistit lokalizační požadavky pro veškeré operace zpracování informací a dat je však značně nepřiměřené a vyhovění tomuto požadavku v takovém rozsahu je z pohledu poskytovatelů cloudových služeb či poskytovatelů informačních systémů technicky neproveditelné. I za předpokladu, že by veškerá data byla uložena výhradně na vymezeném území, jak předpokládá navrhovaná úprava, pro nadnárodní poskytovatele cloudových služeb či jiných informačních systémů není možné zajistit, aby např. v rámci servisní	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		podpory informačního systému přistupovali pracovníci poskytovatele k datům pouze na vymezeném území. Stejným způsobem s požadavky na lokalizaci pracuje cloudová vyhláška, která např. v ID 1.3 přílohy 2 stanovuje, že *„zákaznická data **ve stavu neaktivních dat jsou ukládána** […]“*. **Navrhujeme proto omezit lokalizační požadavky pouze na operaci s informacemi a daty, které zahrnují jejich uchovávání v podobě neaktivních dat.**	
4. ZÚŽENÍ ROZSAHU DOTČENÝCH DAT NA ZÁKAZNICKÁ DATA - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - § 29 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“.	Navrhujeme stanovit, že požadavky na lokalizaci se nevztahují na veškeré informace a data, ale pouze na **zákaznická data**.	V případě, že dojde ke stanovení lokalizačních kritérií, je nepřiměřené, aby se lokalizační požadavky vztahovaly na jakékoliv informace a data, a to bez další specifikace, že se má jednat o vztah k dotčenému systému, resp. regulované službě. Předvídané široké vymezení údajů může při hodnocení dopadů kybernetického incidentu (což je tedy předvídané hodnotící kritérium) znamenat, že veškeré nebo téměř veškeré informace a data budou podléhat lokalizačním požadavkům, což může zcela ochromit regulované subjekty a jejich využívání inovativních technologií, včetně cloudových služeb. Z hlediska kybernetické bezpečnosti regulovaných služeb přitom nelze předvídat, že veškerá data, se	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		kterými může regulovaný subjekt nakládat, by měla požívat stejné ochrany. Rozdílnou úroveň ochrany zpravidla bude vyžadovat samotný obsah a jiný metadata nezbytná pro zajištění provozu. Po vzoru cloudové vyhlášky navrhujeme omezit lokalizační požadavky pouze na vymezenou kategorii dat. Ačkoliv však cloudová vyhláška stanovuje lokalizační požadavky i na tzv. specifické provozní údaje, navrhujeme omezit lokalizační požadavky dle navrhované právní úpravy pouze na zákaznická data. Na rozdíl od zákaznických dat, na nimiž má zpravidla zákazník plnou kontrolu, specifické provozní údaje musí být standardně zpracovávány či ukládány na různých lokacích k zajištění řádného fungování informačního systému. **Navrhujeme proto omezit lokalizační požadavky pouze na informace a data, která naplňují následující definici zákaznických dat**: *"**zákaznickými daty** se rozumí všechna data, která jsou uživatelem nebo administrátorem na straně povinné osoby vložena do informačního a komunikačního systému využívaného pro poskytování regulované služby nebo jsou výsledkem využití takového informačního a komunikačního systému uživatelem*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		v průběhu využívání informačního a komunikačního systému".	
5. VÝJIMKY Z LOKALIZAČNÍCH POŽADAVKŮ - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí".	Navrhujeme doplnit technické výjimky z požadavků na zpracování informací a dat na konkrétním území, resp. tedy, v souladu s připomínkami výše, z požadavků na ukládání zákaznických dat. Tyto výjimky by měly nahradit stávající ustanovení § 29 odstavec 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností. V každém případě však navrhujeme, aby tyto výjimky byly rovněž stanoveny na úrovni zákona o kybernetické bezpečnosti – zde se tedy může jednat o nahrazení výjimky odst. 3 ustanovení *§ X Podmínky lokalizace informací a dat*. *Konkrétní výjimky, které slouží k dosažení technické splnitelnosti,*	Vzhledem ke globální povaze internetu a jednotlivých služeb nelze ve všech případech plně dosáhnout toho, aby data byla bez dalšího zpracovávána jen na předem vymezeném území. Součástí standardní architektury datových úložišť, a tedy nezbytnou součástí kybernetické bezpečnosti služeb a dat je, že data jsou ukládána na diferencovaných lokacích, a to často napříč různými regiony, kde mohou být data např. replikována či jinak zrcadlena. Taková diferenciace a variabilita úložišť zvyšuje dostupnost a integritu těchto dat v případě jakéhokoliv výpadku či narušení služby. Stejné požadavky mohou vznikat v rámci zajišťování (technické) podpory takových služeb, které jsou pro zajištění maximální dostupnost často stavěny na principu „follow-the-sun", tedy mohou být poskytovány z různých regionů napříč světem. Zákonodárce se již obdobnou otázkou zabýval a specificky tyto technické požadavky již reflektoval i v rámci existující právní úpravy katalogu cloud computingu – zejména tedy v rámci výjimek	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	jsou navrženy v rámci komentáře ve vedlejším sloupci.	aplikovatelnosti pravidel katalogu cloud computingu dle § 6l odst. 4 zákona č. 365/2000 Sb., o informačních systémech veřejné správy (dále jen „**ZoISVS**“). Návrh ZKB ani vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností tyto výjimky nijak nezohledňují. Obdobně, jako je tomu u požadavků na služby cloud computingu, by se tak neměly lokalizační požadavky uplatnit na informace a data, která slouží výlučně pro účely stanovené v § 6l odst. 4 ZoISVS. **Navrhujeme proto zakotvení těchto konkrétních výjimek (např. jako nový odstavec 3 ustanovení *§ X Podmínky lokalizace informací a dat:*** „3) Požadavky na lokalizaci zákaznických dat podle tohoto ustanovení se se nevztahují na následující případy: a) data jsou zašifrována v souladu s požadavky [prováděcího předpisu – např. odkaz na § 26 vyhlášky], *[zdroj: navrhovaný §29 odst. 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností]*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		b) zpracování nezbytné ke správě a řešení technických potíží nebo diagnostice programových anebo technických prostředků, případně k zabezpečení nebo přenosu s tím souvisejících signálů a k zajištění odhalování anebo řešení kybernetických hrozeb či incidentů, *[zdroj: § 6l odst. 4 písm. a) ZoISVS]* c) zpracování slouží ke správě nebo využívání prostředků pro elektronickou identifikaci, včetně prostředků využívajících vícefaktorové autentizace, *[zdroj: § 6l odst. 4 písm. b) ZoISVS]* d) zpracování slouží k aktualizace či opravě programového prostředku, *[zdroj: § 6l odst. 4 písm. c) ZoISVS]* e) zpracování slouží ke shromažďování či výměně provozních údajů a jiných údajů o provozu využívaných prostředků, *[zdroj: § 6l odst. 4 písm. d) ZoISVS]*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		f) zpracování slouží k výměně dat na bázi protokolů internetu věcí, nebo *[zdroj: navrhuje se jako nová výjimka]* g) ke zkušebnímu provozu, pokud při něm nebudou využity údaje, které se v daném systému vedou nebo povedou anebo které jsou nebo budou v souvislosti s poskytováním služby využívány. *[zdroj: § 6l odst. 4 písm. e) ZoISVS]*	
6. SJEDNOCENÍ LOKALIZAČNÍCH KRITÉRIÍ S KVALIFIKAČNÍMI KRITÉRII PRO BEZPEČNOSTNÍ ÚROVEŇ - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. - Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací	Navrhujeme sjednotit kvalifikační kritéria pro lokalizaci informací a dat (nyní obsažená v § 29 odst. 2 a 4 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) s kritérii pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computingu, do bezpečnostní úrovně dle Přílohy vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy, resp. pouze nahradit tato kritéria jednotnými referencemi	Navrhujeme sjednocení kritérií pro stanovení lokalizačních požadavků s kvalifikačními kritérii pro bezpečnostní úroveň pro úroveň „4. Kritická“. Kritéria pro požadavky na lokalizaci informací a dat (nyní § 29 odst. 2 a 4 Vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností) se částečně překrývají s kritérii bezpečnostních úrovní (resp. tedy kritérii pro zařazení informačního systému veřejné správy k zajištění jehož provozu má být využíván cloud computing dle Přílohy vyhlášky o bezpečnostních úrovních informačních systémů veřejné správy). Mezi těmito kritérii však existují odchylky, které nejsou jakkoliv zdůvodněné. Za předpokladu, že dojde	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
a dat při zpracování v zahraničí“, - Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy: Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computingu, do bezpečnostní úrovně“.	– takovým způsobem, aby za každé situace byla zachována jednotnost pro kritickou a vysokou úroveň.	k úpravě lokalizačních požadavků tak, aby se vztahovaly jen na kritickou bezpečnostní úroveň, navrhujeme jejich sjednocení, a to ideálně v podobě referencí – tak, aby ani v budoucnu (např. v případě přijímání jakékoliv novely) nedošlo k jejich rozkolu. Navrhujeme, aby tyto požadavky byly převzaty ze stávajícího právního rámce pro určování kritické informační infrastruktury dle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (bod VI. KOMUNIKAČNÍ A INFOMRAČNÍ SYSTÉMY), které tedy byly stanoveny jako kritéria určení pro nejzásadnější systémy, které mají podléhat nejpřísnějším požadavkům na kybernetickou bezpečnost a mají být tedy chráněny v nejpřísnější bezpečnostní úrovni „4. Kritická“.	
7. NESPRÁVNÝ ODKAZ V ODST. § 29 ODST. 3 VYHLÁŠKY O BEZPEČNOSTNÍCH OPATŘENÍCH POSKYTOVATELE REGULOVANÉ SLUŽBY V REŽIMU VYŠŠÍCH POVINNOSTÍ - Vyhláška o bezpečnostních opatřeních poskytovatele	Upravit odkaz v tomto ustanovení na z referovaného „odst. 1“ na odst. 2.	Pokud by nebylo vyhověno výše uvedeným připomínkám a text by zůstal v této vyhlášce, je nezbytné upravit nesprávný odkaz v § 29 odst. 3: *„Povinnost stanovená v ~~odst. 1~~ **odst. 2** se nevztahuje na uchovávání zašifrovaných informací a dat na území […]“*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu vyšších povinností: § 29 odst. 3.			
8. VÝJIMKA PRO LOKALIZAČNÍ POŽADAVKY NA ZPRACOVÁNÍ ŠIFROVANÝCH INFORMACÍ A DAT - Zákon o kybernetické bezpečnosti: § X Podmínky lokalizace informací a dat. Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: § 29 odst. 3.	Navrhujeme upřesnit, že výjimka z lokalizačních požadavků pro zašifrovaná data stanovená v § 29 odst. 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností se vztahuje na zpracování, nikoliv jen uchovávání dat: *„3) Povinnost stanovená v [odst. 2; k tomu viz samostatná připomínka výše] se nevztahuje na **zpracování, včetně** uchovávání, zašifrovaných informací a dat na území […]“*	Výjimka z lokalizačních požadavků, která je v současnosti upravená v § 29 odst. 3 vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností, se vztahuje na **uchovávání** informací a dat zašifrovaných podle § 26 předmětné vyhlášky. Dle důvodové zprávy k této části se má výjimka uplatnit pouze „pro výjimečné situace (např. hrozby konfliktu s cizími státy, válečný stav, přírodní katastrofa velkého rozsahu atp.)“. Při déle trvajících výjimečných stavech je však nezbytné a žádoucí, aby se předmětná výjimka vztahovala i na **jakékoliv zpracovávání**, nikoliv pouze ukládání, zašifrovaných informací a dat, např. k tomu, aby mohl být příslušný informační systém spuštěn i z území jiných států. Limitace na ukládání takových údajů může vést k nežádoucímu narušení funkčnosti systémů a přístupu k datům (a to zejména v krizových situacích, kdy může být naprosto zásadní, aby data byla dostupná, což limitace jejich uložení na jedno území (dokonce pak Českou republiku) může být nežádoucí a škodlivé).	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Z technického hlediska navíc platí, že ačkoliv většina kryptografických algoritmů slouží především k zabezpečení informací a dat ve formě neaktivních dat, v současnosti existují moderní zabezpečovací techniky, které dovedou zabezpečit i v daném okamžiku využívané (tj. zpracovávané) informace a data. Mezi takové technologie patří např. technologie tzv. *confidential computing* či *client-side encryption*. Pokud by tak mělo dojít k zachování lokalizačních požadavků, včetně této výjimky v odst. 3, navrhujeme toto ustanovení upravit tak, aby se tato výjimka vztahovala na jakékoliv **zpracování informací a dat**.	
ZKB, str. 11	Hlášení kybernetických bezpečnostních incidentů	Hlášení bezpečnostních incidentů s původem v kybernetickém prostoru je velmi vágní pojem (a to i s ohledem na vysvětlení pojmů v zákoně – kybernetickým *prostorem digitální prostředí tvořené aktivy umožňující vznik, výměnu a další zpracování informací a dat.*). S uvedenou připomínkou souvisí doplňující otázky: Jakým způsobem může společnost u každého BI zjistit jeho původ? Jak pracovat s incidenty, kdy vektory útoku mohou mít původ v různých oblastech (např. fyzická bezpečnost, bezpečnost osobních údajů atd.), ale celkově se tyto vektory „skládají“ do jednoho útoku.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Hlásí se vše nebo pouze část ve vztahu ke kybernetické bezpečnosti? Zákon se dále dostatečně nevypořádává se situací, kdy se z provozního incidentu stane bezpečnostní incident – jedná se zejména o dodržení lhůt, kdy samotný provozní incident může být detekován v určitý čas a jeho původ v kyberprostoru se zjistí až o několik hodin/dní později. Bude to považováno za porušení oznamovací lhůty?	
ZKB	§X Náležitosti hlášení kybernetických bezpečnostních incidentů Odst. 6 - Obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy stanoví prováděcí právní předpis. [Vyhláška o Portálu NÚKIB]	Náležitosti závěrečné zprávy nejsou ve jmenované vyhlášce obsaženy.	
ZKB, str. 13	§ Informační povinnost poskytovatele regulované služby, odst. 1	Bylo by vhodné specifikovat pojem “ve vhodných případech” a to zejména s ohledem na to, že podle § X [Přestupky] odst. 1, písm. e) se, v případě nesplnění informační povinnosti, jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu. Zároveň se obáváme, zda takto vágní ustanovení nebude klást na povinný subjekt nepřiměřené	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		požadavky a povinný subjekt by tak měl povinnost informovat uživatele o většině i drobných incidentech, což by mohlo negativně ovlivnit dobré jméno i obchodní tajemství povinného subjektu.	
ZKB, str. 13	Informační povinnost poskytovatele regulované služby (odstavec 2):	*„Poskytovatel regulované služby je povinen bez zbytečného odkladu, srozumitelně a transparentním způsobem informovat 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 takové informování možné a vhodné, informuje poskytovatel regulované služby uživatele také o významné kybernetické hrozbě samotné.“* Uvedené ustanovení vyvolává následující dotazy: 1. V zákoně i důvodové zprávě chybí specifikace toho, kdo je uživatel regulované služby (např. v případě výroby elektrické energie jsou uživateli všichni obyvatelé v ČR/Evropě??) 2. Jak poznáme, že daná hrozba je významná a máme o ní komunikovat? Budeme proaktivně všechny „strašit“? Jak se vyhneme nařčení ze šíření poplašné zprávy?	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Jakým způsobem bude naloženo s informováním o incidentu, pokud jeho šetření budou souběžně řešit OČTŘ (jak bude zajištěno, že nebudeme mařit jejich výkon?)?	
ZKB	§ X Výstraha Úřad je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn veřejnost informovat o kybernetickém bezpečnostním incidentu či o porušování povinností daných tímto zákonem, nebo dotčenému orgánu nebo osobě uložit, aby tak učinily samy.	V případě implementace směrnice došlo k vypuštění zásadní části původního ustanovení spočívající v konzultaci s dotčeným subjektem takového kybernetického bezpečnostního incidentu. V tomto případě se tedy jedná o konzultaci se subjektem, který takový incident nahlásil a je nutné konzultovat obsah a formu zveřejnění takového oznámení, aby nedošlo k odhalení případných zranitelnosti a důvěrných informací povinného subjektu, obchodního tajemství, resp. informací které by mohly vést k prohloubení dopadů incidentu, nebo ke vzniku dalšího. S vyzrazením obchodního tajemství nebo důvěrných informací je spojena náhrada škody nebo sankce v rámci obchodně-právních vztahů. Upozorňujeme, že takovéto veřejné oznámení může mít negativní vliv na ochranu vnitřního pořádku a bezpečnost nebo ochranu ekonomiky státu a může být tedy zcela kontraproduktivní a vyvolat zcela neočekávané účinky, resp. opačné účinky (negativní účinky) než je zamýšleno.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Navrhujeme doplnění o nutnost konzultace s dotčeným subjektem a odsouhlasení oběma stranami na obsahu takové veřejné informace. Obdobně jako je formulováno v § 12, odst. 3, Zákona o kybernetické bezpečnosti a o změně souvisejících zákonů v platném znění.	
ZKB, str. 14	§ Reaktivní protiopatření	Bylo by vhodné specifikovat, jaký charakter a rozsah může povinnost uložená Úřadem mít, a to zejména s ohledem na možné finanční náklady povinného subjekty v těch případech, kdy by byla požadována implementace konkrétního technického opatření. Obáváme se, že takto vágní ustanovení by mohlo v budoucnu zapříčinit, že budou na povinný subjekt kladeny nepřiměřené požadavky a nebudou pro Úřad existovat mantinely, v kterých takové reaktivní protiopatření vydat.	
ZKB, str. 7 a 8	§ Hlášení údajů poskytovatelem regulované služby 4) Poskytovatel regulované služby je povinen hlásit změny pouze těch údajů podle odstavce 2, které nejsou referenčními údaji vedenými v základních registrech, a to nejpozději do 10 dnů od jejich změny.	- Referenční údaje nejsou konkrétně popsány. - Mělo by být součástí vyhlášky o Portálu NÚKIB, které konkrétní údaje mají být hlášeny při změně údajů dle odst. 2 (ve vyhlášce o Portálu NÚKIB ale asi je uvedeno s odkazem na § 26 zákona č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů (poznámka č. 2, str. 2, § 2 Osoby přistupující do Portálu NÚKIB).	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, str. 8	Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby	5) U těch aktiv, která ještě nebyla identifikována a určena podle odstavce 1 nebo zahrnuta do stanoveného rozsahu podle odstavce 4, se má za to, že jsou součástí stanoveného rozsahu, dokud tyto změny nejsou zahrnuty v procesu identifikace a určování organizačních částí orgánu nebo osoby a aktiv tvořících rozsah řízení kybernetické bezpečnosti podle odstavce 1 a není o nich veden dokumentovaný záznam podle odstavce 3. Bylo by možné upřesnit, jak je to přesně myšleno?	
ZKB, str. 9 a 10	§ Seznam bezpečnostních opatření poskytovatele regulované služby - Odst. 2, písm. a) a bod iv) - řízení bezpečnostní politiky a bezpečnostní dokumentace - Odst. 3, písm. a) a bod iv) - řízení bezpečnostní politiky a dokumentace	○ Odstavec 3 písm. a) a bod iv) neobsahuje slovo bezpečnostní dokumentace. Mělo by být shodně se zněním v odst. 2. ○ V zákoně a vyhláškách se nevyskytuje použití formulace „bezpečnostní politika a bezpečnostní dokumentace“ jednotně, v některých případech je slovo bezpečnostní ve vazbě na dokumentaci vypuštěno, tzn., je tak jako je uvedeno v odst. 3.	
ZKB, str. 11 a 12	§ Náležitosti hlášení kybernetických bezpečnostních incidentů Odst. 6 - Obsah a způsob hlášení kybernetického bezpečnostního incidentu, a náležitosti závěrečné zprávy stanoví prováděcí právní předpis. *[Vyhláška o Portálu NÚKIB]*	Vyhláška o Portálu NÚKIB neosahuje popis závěrečné zprávy o řešení kybernetického bezpečnostního incidentu	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, str. 12	§ X Zvládání kybernetických bezpečnostních incidentů 1) Úřad nebo Národní CERT poskytne bez zbytečného odkladu, nejpozději do 24 hodin od obdržení prvotního hlášení podle § X [Náležitosti hlášení kybernetických bezpečnostních incidentů], poskytovateli regulované služby své vyjádření ke kybernetickému bezpečnostnímu incidentu. § X Náležitosti hlášení kybernetických bezpečnostních incidentů, odst. 3	Co se stane, pokud NÚKIB nebo CERT nebudou mít kapacitu v případě velkého množství hlášených incidentů reagovat do 24 hodin? Lhůta reakce NÚKIB do 24 hodin od prvotního hlášení poskytovatelem regulované služby je stanovena pouze v § X Zvládání kybernetických bezpečnostních incidentů. Považujeme za vhodné tuto lhůtu uvádět současně, případně odkazem, i v § X Náležitosti hlášení kybernetických bezpečnostních incidentů, kde jsou uvedeny lhůty pro poskytovatele regulované služby.	
ZKB, str. 31	Evidence vedené Úřadem Odst. 4) Zaměstnanci České republiky zařazení k výkonu práce v Úřadu jsou vázáni povinností mlčenlivosti o údajích z evidencí podle odstavce 1 písm. b) až e). Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu. Ředitel Úřadu může tyto osoby zprostit povinnosti mlčenlivosti, s uvedením rozsahu údajů a rozsahu zproštění.	Evidence pod písm. a) poskytovatelů regulovaných služeb a jejich hlášených údajů a f) provedených kontrol a protokolů o kontrole se do mlčenlivosti nezahrnují?	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB, str. 35	Zpracování osobních údajů	Bylo by vhodné zvážit, zda je nutné výjimku z pravidel stanovených v GDPR definovat takto široce, zejména v oblasti stanovení výjimky z účelů, pro které byly osobní údaje shromážděny.	
ZKB, str. 35	Zpracování osobních údajů Odst. 2 Úřad, provozovatel Národního CERT a inspektoři při zpracování osobních údajů, na které se vztahuje přímo použitelný předpis Evropské unie upravující ochranu osobních údajů, písm. b) mohou v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny.	Pro jaké účely je to možné, uvedeno „jiné“ účely.	
ZKB, str. 38	§ X Kontrola vykonávaná inspektory 1) Inspektor vykonává kontrolu v oblasti kybernetické bezpečnosti v rozsahu stanoveném tímto zákonem. Při výkonu kontroly inspektor zjišťuje, jak poskytovatel regulované služby v režimu nižších povinností plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržuje prováděcí právní předpis v oblasti kybernetické	Znamená to, že inspektoři budou vykonávat kontrolu jen regulovaných subjektů s nižšími povinnostmi? A NÚKIB bude vykonávat kontrolu všech regulovaných subjektů v rozsahu vyšších povinností?	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	bezpečnosti [Vyhláška o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu nižších povinností].		
ZKB, str. 41	§ X Nápravná opatření 1) Zjistí-li Úřad při kontrole nedostatky nebo vyplývají-li tyto nedostatky z obsahu protokolu o kontrole provedené inspektorem, může Úřad uložit kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určit jakým způsobem. Úřad může uložit povinnost oznámit provedení nápravného opatření a jeho výsledek ve stanovené lhůtě. Poskytovatel regulovaných služeb hlásí provedení nápravného opatření prostřednictvím Portálu NÚKIB; náležitosti a způsob hlášení stanoví prováděcí právní předpis [Vyhláška o Portálu NÚKIB].	Znamená to, že inspektor nestanovuje doporučené opravné prostředky a tato odpovědnost jde vždy za NÚKIB?	
ZKB	Přestupky, odst. 1, písm. a)	Bylo by vhodné zvážit, zda není požadavek na bezchybné určení a identifikaci aktiv a organizačních částí formulován příliš tvrdě, obzvlášť v případě povinných subjektů s rozsáhlou a komplikovanou ICT	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		infrastrukturou, a to zejména s ohledem na to, že se jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu. Částečným řešením by mohlo být zpřesnění pojmu „bezchybné určení a identifikace aktiv“, resp. odstupňování výše pokuty podle toho, jak závažné by případné chybné určení bylo.	
ZKB	Přestupky, odst. 15	Bylo by vhodné zvážit, zda stanovené výše a rozsahy uvedených pokut nejsou příliš tvrdé a široké a zda nenechávají příliš volný prostor pro diskreční pravomoc Úřadu, a to bez konkrétně formulovaných kritérií pro ukládání takto, pro povinné subjekty, citlivých sankcí.	
ZKB	§ Vymezení pojmů 1 a) *aktivem primární aktiva a podpůrná aktiva relevantní pro shromažďování, nakládání, uchovávání, užívání, sdílení, rozšiřování nebo jiné zpracování informací a dat v elektronické podobě*	Definování relevantnosti aktiva pro zpracování informací a dat pouze v elektronické podobě je nedostatečné pro případy, kdy informace a data nebudou zpracovávány elektronicky, avšak bude na ně potřeba uplatňovat bezpečnostní opatření z pohledu regulované služby. Příkladem může být např. klasifikace informací či způsoby likvidace dat a informací, kde jsou definovány bezpečnostní zásady i pro listinné nosiče informací. 2 a-j) jelikož bylo provedeno značně rozsáhlé rozšíření pojmů oblasti kybernetické bezpečnosti, bylo by vhodné definovat i samotný pojem „kybernetická bezpečnost“, „kybernetický bezpečnostní incident	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		s významným dopadem“ a „uživatel regulované služby“.	
ZKB	§ Vymezení pojmů, odst. 2, písm. i)	Bylo by vhodné specifikovat pojem “významný dodavatel” natolik, aby výklad tohoto pojmu poskytoval povinnému subjektu jasné vodítko pro určení dodavatelů, spadajících do této kategorie, a to zejména s ohledem na skutečnost, že podle § X [Přestupky] odst. 1, písm. b) se, v případě nesplnění povinnosti při jejich identifikaci, jedná o přestupek, za který lze podle odst. 15, písm. a) uložit nejvyšší možnou pokutu.	
ZKB	§ Speciální úprava předání informací a dat od významného dodavatele	Bude tento § uplatňován i u zahraničních významných dodavatelů? § Vzájemná součinnost s členskými státy Evropské unie (str. 36) definuje v odstavci 1, písm. b, pouze „jiné úkony“. Lze tedy chápat stanovisko v odůvodnění (str. 43): *Odst. 1 řešeného ustanovení zakotvuje základní způsoby spolupráce a pomoci zmíněné v čl. 37 odst. 1 a 2 směrnice NIS2, tedy sdílení informací, koordinaci a spolupráci při provádění opatření v oblasti dohledu a vymáhání,* jako pravomoc Úřadu i v těchto případech (předání informací a dat od významného dodavatele)?	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB	Příliš široká definice „významného dodavatele“ dle návrhu kybernetického zákona (příloha 1a).	Z definice není jasné, o jaké dodavatele se má jednat: „významným dodavatelem každý, kdo s poskytovatelem regulované služby vstupuje do právního vztahu, který je významný z hlediska stanoveného rozsahu řízení kybernetické bezpečnosti.“	
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Přehodnocení institutu OOP jako prostředku pro omezení dodavatelského řetězce. Případné doplnění tohoto procesu o konkrétní procesní kroky NÚKIB do ZKB. Zajištění právních jistot subjektům, kteří vstupují do procesu Mechanismu. Přezkoumatelnost vydaného OOP.	NÚKIB v návrhu zákona předkládá jako prostředek Mechanismu OOP, který může mít v případě využití pro takový účel některé nedostatky. Zároveň z důvodové zprávě je uváděno: „Stanovit omezení jiným způsobem, například rozhodnutím Úřadu, by vyžadovalo, aby Úřad disponoval významně větším rozsahem informací o bezpečnostně významných dodávkách, než vyžaduje předkládaná podoba návrhu“. Z uvedeného by však vyplývalo, že NÚKIB si je vědom, že koná bez znalosti předmětu posuzování samotného OOP. Nelze se však domnívat, že by mohlo dojít k posouzení něčeho, o čem posuzující subjekt nemá dostatek informací. Odůvodnitelnost OOP jako prostředku, který je určen neurčitému počtu adresátů nepovažujeme taktéž za adekvátní, a to už z důvodu toho, že NÚKIB je povinen vést databázi poskytovatelů regulovaných služeb. Z takového seznamu je v případě potřeby jistě možné zajistit konkrétní okruh adresátů.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Institut OOP v omezené formě, kterou NÚKIB předkládá v návrhu zákona, mimo jiné neumožňuje subjektům podávat námitky jako účastníkům řízení. Zároveň i s ohledem na znění ostatních připomínek akcentujeme, že OOP vydává NÚKIB sám a nepodléhá schválení např. správním orgánům a institucím, kterým náleží gesce ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu, jak je v zákoně a vyhláškách často zmiňováno. Ve znění § X Prověřování rizik spojených s dodavatelem ZKB není dostatečným způsobem popsán proces, kterým NÚKIB dojde k závěrům shrnutým v OOP. Textace „Úřad shromažďuje a vyhodnocuje informace a data“ není dostatečným popisem procesních kroků, které bude NÚKIB činit a nezakládá ani předpoklad, že návrh znění OOP bude zpětně konzultován s orgány, které NÚKIBu předkládaly informace a bude zároveň podléhat schválení některých z nich. Součástí celého procesu by měla být bezpodmínečně analýza rizik a dopadová analýza nákladů a výnosů takového opatření. Příkladem obdobného procesu, který je již praxí ověřený, může NÚKIBu sloužit např. proces analýzy relevantních trhů ČTÚ. Zásadním nedostatkem OOP je ovšem nemožnost podání opravného prostředku. V případě takto	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		významného omezení tržního prostředí považujeme za zásadní, aby se dotčené subjekty mohly bránit proti vydání takového opatření jinou, než pouze soudní cestou. Soudní přezkum vydaného OOP je s ohledem na lhůty výběrového řízení dodavatele a jeho prověřování pro interní účely a celého procesu kontrakce a dodávky nových technologií nedostačující. Aplikuje se zde princip ex nunc, což v tomto případě znamená, že dotčená osoba bude muset po vydání OOP konat okamžitě, aby stihla případnou lhůtu pro výměnu/vyřazení technologií omezeného/zakázaného dodavatele. Proto kontrakty s omezeným/vyřazeným dodavatelem v případě zrušení OOP soudem již nebude možné obnovit.	
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce Vyhláška o nepominutelných funkcích daného rozsahu	Fixace cyklu dožití technologie v zákoně	Zákon, a především jeho odůvodnění pracuje s předpokladem, že lhůty pro vykonání povinností plynoucích z OOP budou povinným osobám stanovovány s ohledem na dobu životnosti jednotlivých prvků sítě a celkově jejich životní cyklus. Vyžadujeme zafixování takového tvrzení v samotném zákoně, a to případně i pevnou nejkratší dobou vykonavatelnosti povinností odrážející dobu takové životnosti, tj. minimálně 5 let. Kdy NÚKIB v OOP může tuto lhůtu jen	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		prodloužit, avšak ne zkrátit. Dojde tak k významně lepší předvídatelnosti podnikatelského prostředí.	
ZKB Mechanismus prověřování bezpečnosti dodavatelského řetězce	Zavedení kompenzací státu za zásah do tržního prostředí.	Mechanismus bude výrazným zásahem do podnikatelského prostředí v telekomunikační sféře. Důsledkem takové regulace může nastat nedostatek kvalifikovaných pracovních sil v případě, že OOP bude plošně aplikováno na celý sektor. Dalším důsledkem může být nedostatečná úřední kapacita při povolování změn v území. Dále může dojít k vendor lock-in – takové kroky jsou navíc v rozporu s 5G EU Toolboxem, jehož jednou z hlavních priorit je diverzifikace dodavatelského řetězce. V neposlední řadě bude mít takové opatření významný finanční dopad na podnikatelské prostředí. Zavedení kompenzačních prostředků v případě, že dojde na základě konání NÚKIB k omezení tržního prostředí považujeme za nezbytné. Jedná se o případy, kdy povinná osoba mechanismu bude omezena ve svém podnikání a budou jí způsobeny náklady, se kterými logicky nemohla předem počítat a nebyly nastaveny dostatečné lhůty pro výměnu realizovaných/zasmluvněných dodávek.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
ZKB § X Výjimky z omezení rizik spojených s dodavatelem	Větu první v odst. 2) navrhujeme upravit takto „Řízení o povolení výjimky podle odstavce 1 lze zahájit pouze na žádost.“	Všechny přímo dotčené osoby povinné mechanismu musí mít rovné právo požádat o výjimku a následný přezkum rozhodnutí NÚKIB, což nelze nahradit rozhodováním jen ze strany NÚKIB a tím vyloučením rovného práva před zákonem.	
ZKB Řízení dodavatelů a vztah k zadávání veřejných zakázek: „…nelze považovat za nezákonné omezení hospodářské soutěže“	Změna formulace na vyvratitelnou právní domněnku: „*Má se za to, že zohlednění požadavků vyplývajících z bezpečnostních opatření není nezákonným omezením hospodářské soutěže nebo neodůvodněnou překážkou hospodářské soutěže*“.	Riziko zneužití za účelem vyloučení dodavatelů, s nimiž nebude ochota vstoupit do smluvního vztahu z jiného důvodu než bezpečnostních opatření.	
ZKB Speciální úprava předání informací a dat od významného dodavatele	Bližší specifikace informací a dat „informace a data související s provozem aktiv soužících k poskytování regulované služby, **kterými významný dodavatel disponuje a které nejsou předmětem ochrany podle autorského práva**“. Doplnění explicitní úpravy pro situaci, kdy významný dodavatel požadovanými informacemi a daty	Již v současné době působí aplikační problémy nedostatečné vymezení okruhu dat a informací spadajících pod povinnost vydání podle § 6a odst. 2 a 3 ZKB. Navržená úprava představuje minimální zpřesnění na informace a data, kterými významný dodavatel disponuje. Pro případ požadavku takových informací a dat, kterými naopak nedisponuje by mu měla náležet odměna v podobě účelně vynaložených nákladů. Návrh ZoKB to implicitně řeší v odstavci 4 dotčeného ustanovení. V rámci vyváženosti je však nutné dikci	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	nedisponuje, ale bude požadováno jejich opatření a následné vydání: „Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby, přesto bude účelné uložit jeji opatření a vydání, je poskytovatel regulované služby povinen uhradit významnému dodavateli v této souvislosti účelně vynaložené náklady.“	odst. 4, která chrání poskytovatele významné služby, zakotvit rovněž ochranu významných dodavatelů, a to v podobě explicitního závazku na nárok na odměnu za poskytnuté plnění. Významný dodavatel by rovněž neměl být nucen předávat informace a data, která představují dílo ve smyslu autorského zákona. Je na poskytovateli regulované služby, aby si vhodně ošetřil licenční problematiku v soukromoprávní smlouvě. NUKIB by svými zásahy neměl suplovat zanedbání těchto otázek ve smlouvě. Ve svém důsledku může bezbřehá povinnost významného dodavatele předat data a informace vést k rezignaci poskytovatelé regulované služby, jako zadavatelů veřejných zakázek, na ošetření problematiky licenčních ujednání, exitového plánu apod.	
Příloha vyhlášky o kritériích rizikovosti dodavatele, kritérium 10 a 11	Bez náhrady vypustit, alternativně navázat na pravomocné rozhodnutí soutěžního orgánu či soudu.	Zvolená formulace „vykazuje znaky … „ je naprosto vágní, pročež dává příliš široký prostor pro správní uvážení NÚKIB, a to navíc v oblastech, které jsou svěřeny do pravomoci soutěžních orgánů (v případě hospodářské soutěže) či civilních soudů (v případě péče řádného hospodáře).	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
Vyhláška o regulovaných službách	§ 4 Kritéria pro určení regulované služby	Pokud příslušný subjekt **nebude** určený jako poskytovatel regulované služby dle přílohy Vyhlášky a také ani Úřadem, avšak z povahy podnikatelských činností subjektu (např. dopadů do významných služeb státu či jiných regulovaných služeb) bude patrná jeho důležitost pro „určení“, je povinností příslušného podnikatelského subjektu informovat Úřad o potřebě přehodnocení/zvážení „určení“ do regulované služby?	
Vyhláška o regulovaných službách	Podle bodu 7.4 písm. b) návrhu vyhlášky o regulovaných službách („Vyhláška“) „Výrobce motorových vozidel, přívěsů a návěsů ve smyslu oddílu 29 klasifikace CZ-NACE je poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí autobusy“.	Domníváme se, že kritérium „sériové výroby autobusů“ nereflektuje charakter výroby autobusů v podmínkách České republiky, která je svým charakterem většinově výrobou zakázkovou, nikoliv sériovou. Každá výrobní zakázka má konkrétního zákazníka, přičemž zákaznické požadavky vykazují materiální odlišnosti ve vazbě na konkrétní trh/zemi určení (např. specifické úpravy pro konkrétní klimatické podmínky), konkrétní typ dopravy (např. modifikace obsaditelnosti a rozmístění sedadel produktu pro městskou, příměstskou nebo meziměstskou dopravu), konkrétní dopravní systém (specifické požadavky na odbavovací, informační systém vozidla či adaptace na konkrétní dispečerský systém daného dopravního systému/zákazníka).	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Obvyklá série identických vozidel tak čítá v průměru cca 10 ks. Díky zakázkovému charakteru výroby s datem dodání dle požadavků konkrétního zákazníka je možné negativní dopady na výrobní proces způsobené případnými kybernetickými bezpečnostními incidenty (např. případný dopad na časový harmonogram výroby) adresovat v rámci komunikace s těmito jednotlivými zákazníky. Výroba autobusů představovala v roce 2020 pouze 0,4% výroby motorových vozidel v České republice (celkem bylo vyrobeno 5 070 autobusů). Jak již bylo uvedeno, významní výrobci autobusů v České republice vyrábí většinově customizované typů autobusů, a to ve stejných výrobních halách. Je tedy nutné mít flexibilní pracoviště. Z tohoto důvodu nejsou ve výrobě používány počítačově řízené výrobní linky, ani velké série polotovarů či výrobků (výrobci autobusů nejsou závislí na elektronicky řízených linkách ani robotech). Z výše uvedených důvodů si dovolujeme navrhnout, aby kritérium sériové výroby autobusů pro určení poskytovatele regulované služby v režimu vyšších	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		povinností, které jde nad rámec směrnice NIS 2, bylo z návrhu Vyhlášky odstraněno.	
Příloha k vyhlášce o regulovaných službách Kritéria pro identifikaci regulované služby, bod 7.4. Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů	Stanovit režim nižších povinností pro poskytovatele v případě, že vyrábí sériově osobní motorová vozidla	Aktuální návrh vyhlášky o regulovaných službách stanovuje pro výrobce motorových vozidel, který vyrábí sériově osobní motorová vozidla režim vyšších povinností dle ZKB. Tím navyšuje požadavky, které vyplývají pro takového výrobce ze směrnice NIS 2. Směrnice NIS 2 totiž výrobce motorových vozidel zařazuje do kategorie důležitých subjektů, tj. ekvivalentu subjektů v režimu nižších povinností. Máme za to, že důležitým aspektem při transpozici směrnice do českého práva je významně se neodlišovat od ostatních členských států Evropské unie. V případě, že by na výrobce motorových vozidel byly v České republice kladeny vyšší nároky než v jiných členských státech Evropské unie, může toto mít zásadní negativní dopad na český automobilový trh. Existuje nezanedbatelné riziko, že by kvůli takto zásadně přísnější regulaci čeští výrobci byli nuceni promítnout náklady vyplývající ze zabezpečení vyššího režimu povinností do finální ceny produktu. Čeští výrobci by se tak mohli stát ve srovnání se zahraničními výrobci méně konkurenceschopní. Zároveň je potřeba zmínit, že pro český sektor výrobců motorových vozidel je zásadní co největší shoda	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		s právní úpravou v Německu vzhledem k majetkovému i funkčnímu propojení českého automobilového sektoru s německým. Proto pokud se německý zákonodárce rozhodne ponechat výrobce motorových vozidel v režimu nižších povinností, je velmi žádané, aby takto postupoval i český zákonodárce. NÚKIB uvádí jako odůvodnění pro zařazení výrobců motorových vozidel do režimu vyšších povinností zásadní ekonomický význam společností provozujících sériovou výrobu osobních motorových vozidel pro Českou republiku. Tento argument nerozporujeme, nicméně domníváme se, že není vhodné znevýhodnit určitou skupinu výrobců pouze pro to, že jejich ekonomická činnost tvoří významnou část české ekonomiky. Naopak by měl český zákonodárce velmi pozorně přistupovat k tomu, aby nestanovoval nepřiměřeně přísné požadavky, které v důsledku mohou tento ekonomicky velmi důležitý sektor v České republice poškodit.	
Příloha k vyhlášce o regulovaných službách Bod 8.3. *Distribuce potravin* části 8. *Potravinářský průmysl*	Za slova „Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4]“ vložit slova „***vykonávající činnost velkoobchodní distribuce“***.	Působnost směrnice NIS2 jako takové je upravena ve článku č. 2 směrnice NIS2, kde je stanoveno, že se *tato směrnice … vztahuje na veřejné a soukromé subjekty, jejichž druhy jsou uvedeny v příloze I nebo II a které jsou považovány podle článku 2 přílohy doporučení 2003/361/ES za střední podniky, nebo které překračují*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	Úplné znění po přijetí změn: Potravinářský podnik podle přímo použitelného předpisu Evropské unie[4] **vykonávající činnost velkoobchodní distribuce** je poskytovatel regulované služby v režimu nižších povinností, v případě, že je velkým podnikem nebo středním podnikem.	*stropy pro střední podniky stanovené v odstavci 1 uvedeného článku a které poskytují služby nebo vykonávají činnosti v rámci Unie.* Přičemž příloha č. 2, která se věnuje kritickým odvětvím, ve svém bodě č. 3 upřesňuje, že směrnice NIS2 dopadá na ***potravinářské podniky*** *ve smyslu čl. 3 bodu 2 nařízení Evropského parlamentu a Rady (ES) č. 178/2002 (3),* ***které se zabývají velkoobchodní distribucí a průmyslovou výrobou a zpracováním****.* V rozporu se směrnicí NIS2 je působnost v novém zákoně o kybernetické bezpečnosti stanovena šířeji. Nový zákon o kybernetické bezpečnosti, stanovil působnost na základě tzv. regulovaných službáeb a jejich poskytovatů, kdy regulovanou službou se rozumí *služba, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a k jejímuž poskytování jsou používána aktiva.* Kritéria pro jednotlivé poskytovatele regulovaných služeb a regulované služby jako takové, jsou stanovena prostřednictvím Vyhlášky, v rámci, které však byl vypuštěn požadavek velkoobchodní distribuce a v bodech 8.1. přílohy Vyhlášky aktuálně stojí jen, že distribucí potravin jako regulované služby se rozumí „***Potravinářský podnik*** *podle přímo použitelného předpisu Evropské unie je poskytovatel*	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		*regulované služby v režimu nižších povinností, **v případě, že je velkým podnikem nebo středním podnikem**.“* Návrh nového zákona o kybernetické bezpečnosti a navazující návrh Vyhlášky předložené NUKIB rozšiřuje oproti směrnici NIS2 působnost na všechny velké a středně velké podniky vyrábějící, zpracovávající či distribuující potraviny, a to bez ohledu, zda se jedná o velkoobchod nebo maloobchod. Toto rozšíření působnosti, které je taktéž v rozporu se zněním samotné směrnice NIS2, není úměrné rizikům a může vést k velmi vysokým a zbytečným nákladům na dodržování předpisů. Takto široce zvolená oblast působnost by znamenala pro povinné společnosti nezanedbatelné náklady spojené s dodržováním předpisů, přestože fakticky nejsou "kritické" (dle výkladu směrnice NIS2) pro lokální zásobování potravinami. Navrhujeme proto upravit definici regulované služby, aby dopadala v případě distribuční činnosti pouze na velkoobchodní distribuci.	
Příloha k Vyhlášce o regulovaných službách	Upřesnění bodu 16.11 poskytovatel řízené služby (MSP)	Zda stačí při naplnění požadavku regulované služby dle 16.11 se registrovat pouze jednou nebo je nutno registrovat každého zákazníka nebo dokonce pro každý	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		systém zákazníka (např. zákazník má tři IS KII), ve kterém tuto službu poskytují.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	§ 2 Vymezení pojmů *j) vrcholovým vedením osoba nebo skupina osob, které řídí povinnou osobu, nebo statutární orgán povinné osoby,*	Jak je pojem vrcholové vedení myšlen ve vztahu např. ke koncernovému řízení či mateřské/dceřiné společnosti? Toto zejména z pohledu některých povinností dle § 5, které jsou v některých případech vhodnější realizovat z úrovně vrcholového vedení např. koncernu a v některých případech z pohledu samotného poskytovatele regulované služby. Dle konzultace s NÚKIB tento souhlasí s využitím jednotného systému řízení v rámci ekonomického uskupení (např. koncern), tzn. vrcholové vedení představuje vedení každé povinné osoby, nicméně některé jeho povinnosti lze přenést (na základě např. smlouvy apod.) na mateřskou společnost, a to včetně zastoupení vrcholového vedení ve výboru pro řízení kybernetické bezpečnosti.	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností	§4 Systém řízení bezpečnosti informací, odst. 1, písm. k)	Zde předpokládáme, že došlo k chybě a toto ustanovení nemá odkazovat k písm. e), ale nejspíše k písm. d).	
Vyhláška o bezpečnostních opatřeních poskytovatele	§ 5 Povinnosti vrcholového vedení	Umožnit outsourcing/pověření výkonem konkrétních povinností nad rámec obecné odpovědnosti za „zajištění“ těchto činností na osobu odlišnou od	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
regulované služby v režimu vyšších povinností		vrcholového vedení (pro účely podnikatelských seskupení není praktické, aby tyto povinnosti vykonávali členové vrcholového vedení v každé povinné osobě v rámci seskupení). Zejména se tato připomínka týká o § 5 odst. 1 písm. a), h), i) a j) (v ostatních případech vnímáme, že možnost outsourcingu je již obsažena ve formulaci „zajistí“) a odst. 2	
Kritéria bezpečnostních úrovní a kvalifikační kritéria pro lokalizaci dat Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností: Část třetí „Lokalizace informací a dat při zpracování v zahraničí“. Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy: Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu	Navrhujeme nahradit kritéria pro bezpečnostní úroveň „4. Kritická“ odkazem na existující kritéria pro určení kritické informační infrastruktury dle nařízení vlády č. 432/2010 Sb.	Ke kritériím pro bezpečnostní úrovně si dovolujeme zopakovat připomínky, které jsme předkládali k návrhu původní vyhlášky. Bezpečnostní úroveň „4. Kritická“ má být určena pro nejvýznamnější informační systémy České republiky, které jsou (jak předvídá důvodová zpráva) zároveň klíčové pro bezpečnostní zájmy státu. Proto nejvyšší bezpečnostní úroveň (tj. „4. Kritická“) musí zahrnovat pouze nejvýznamnější a nekritičtější informační systémy. V opačném případě může docházet k nežádoucímu výkladovému rozšiřování těchto kritérií, což může vést k uzavření trhu se službami cloud computingu – tj. došlo by k nežádoucímu rozšiřování služeb cloud computingu, které by mohly být poskytovány pouze státním poskytovatelem cloud computingu, čímž by došlo k vyřazení komerčních služeb z trhu. Z tohoto důvodu je nezbytné, aby	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
má být využíván cloud computingu, do bezpečnostní úrovně“		veškerá infrastruktura zařazená do této bezpečnostní úrovně byla co nejužším způsobem vázána na bezpečnost státu a tedy na prvky kritické infrastruktury a aby její stanovení podléhalo přísnému procesnímu režimu za účasti všech dotčených složek státu, podobně jako je tomu nyní u prvků kritické infrastruktury. Pro určování prvků kritické infrastruktury přitom existuje daný postup podle zákona č. 240/2000 Sb., krizový zákon, a souvisejícího nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. Tímto předpisem by nemělo docházet k vytváření nového procesu určování těchto kritických prvků, které jsou zásadní pro fungování státu, ale pouze k provázání s již existujícími pravidly. Navrhujeme proto, aby bylo stanoveno, že dopady kybernetického bezpečnostního incidentu musejí mít zásadní vliv na řádné fungování takto určeného prvku kritické infrastruktury, kde takový zásadní vliv by pak měl být přímo navázán na nařízení vlády č. 432/2010 Sb. Alternativně by pak bylo možné stanovit, že kybernetický incident (jakožto zvažované kritérium dopadu) může způsobit závažné omezení řádného fungování kritické informační infrastruktury, čímž by	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bylo vyjasněno, že kybernetický incident musí mít zásadní dopad pro fungování České republiky. Podle navrhovaných kritérií by bylo možné podstatnou část informační infrastruktury veřejné správy vyhodnotit jako splňující podmínky nejvyšší (4. Kritická) nebo druhé nejvyšší (3. Vysoká) bezpečnostní úrovně a tím zcela znemožnit nebo výrazně omezit využívání cloudových služeb v České republice. Úzké a přísné vymezení kvalifikačních kritérií, včetně procesních záruk v rámci způsobu určování, jsou rovněž zásadní s přihlédnutím ke zvažovaným lokalizačním požadavkům (jejichž kritéria se značně překrývají s bezpečnostními úrovní „4. Kritická“ i „3. Vysoká"). Pokud by lokalizační požadavky byly přes jejich nesoulad s harmonizačními záměry EU ponechány, je nezbytné, aby se vztahovaly jen na nejzásadnější a nejkritičtější systémy České republiky. Toto vymezení by tedy mělo platit i pro případné lokalizační požadavky, které by měly být na vymezení kritické bezpečnostní úrovně přímo navázané.	
Ekonomická kvalifikační kritéria Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších	Navrhujeme: - nahradit částku 1 000 000 Kč uvedenou ve sloupci H. Finančního modelu v Příloze	Nad rámec nezbytného zúžení kvalifikačních kritérií pro kritickou bezpečnostní úroveň (výše) rovněž navrhujeme významné navýšení finančních limitů ekonomických dopadových kritérií.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
povinností, § 29 odst. 2 písm. e) a odst. 4 písm. g) Vyhláška o bezpečnostních úrovních informačních systémů veřejné správy, Příloha „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing do bezpečnostní úrovně“, Sloupec H. Finanční model, Úroveň 3 – Vysoká a 4 - Kritická	„Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud computing, do bezpečnostní úrovně“, pro Úroveň 3 – Vysoká částkou alespoň ve výši 50 000 000 Kč [pozn. padesetinásobek navrhované částky]. Pokud by (navzdory k připomínkám výše) došlo k zachování ekonomického kritéria pro kritickou bezpečnostní úroveň, navrhujeme rovněž: - nahradit částku 10 000 000 Kč uvedenou ve sloupci H. Finančního modelu v Příloze „Úrovně a oblasti dopadu pro zařazení informačního systému veřejné správy, k zajištění jehož provozu má být využíván cloud	Zvýrazněné finanční limity pro zařazení do bezpečnostní úrovně “vysoká” nebo “kritická” (pokud by byly zachovány) považujeme za příliš nízké. Téměř jakýkoli bezpečnostní incident i v malé nebo středně velké společnosti může teoreticky mít tento finanční dopad, zejména pokud se započítají i případné ztráty související se škodou na pověsti a další související ztráty. Vzhledem k tomu, že kritéria jsou alternativní (tedy stačí splnění kteréhokoli z nich) a tomu, že se jedná o nejvyšší možnou představitelnou škodu (“kybernetický bezpečnostní incident může vést k finančním ztrátám přesahujícím”) by toto kritérium vedlo ke kvalifikaci většiny informačních systémů, včetně všech systémů veřejné správy do kategorií Vysoká a Kritická. Tím by dělení do kategorií zcela pozbylo smyslu a všechny systémy by byly předmětem značně vyšších bezpečnostních požadavků předvídaných pro nejvyšší bezpečnostní úrovně. Navrhujeme proto zvýšení těchto finančních kritérií odpovídajícím způsobem. Obdobné odůvodnění platí pro kategorizaci pro účely přísných lokalizačních kritérií.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	computing, do bezpečnostní úrovně“, pro Úroveň 4 – Kritická alespoň částkou alespoň ve výši 200 000 000 Kč [pozn. dvacetinásobek navrhované částky]. Pokud by (navzdory k připomínkám výše) došlo k zachování lokalizačních požadavků, navrhujeme rovněž následující úpravy: - nahradit částku 1 000 000 Kč uvedenou v § 29 odst. 4 písm. g) částkou alespoň ve výši 50 000 000 Kč [pozn. padesetinásobek navrhované částky]; nahradit částku 10 000 000 Kč uvedenou v § 29 odst. 2 písm. e) částkou alespoň ve výši 200 000 000 Kč [pozn. dvacetinásobek navrhované částky];		
MAPOVÁNÍ BEZPEČNOSTNÍCH POŽADAVKŮ	Stanovit, že jednotlivé bezpečnostní požadavky lze splnit prostřednictvím (mezinárodní) bezpečnostní	Předkládaná úprava jednotlivých „bezpečnostních“ vyhlášek (především tedy vyhlášky v režimu vyšších povinností) přináší velmi komplexní set bezpečnostních	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
- Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	certifikace, jako je např. ISO 27001, 27017 a 27018. Na úrovni jednotlivých vyhlášek (např. formou poznámek pod čarou), jejich důvodových zpráv a/nebo samostatného doprovodného dokumentu navrhujeme namapovat požadovaná bezpečnostní opatření s již existujícími bezpečnostními opatřeními podle mezinárodních bezpečnostních standardů (zejména ISO řady 27xxx) či existující vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti.	opatření. Bez detailní technické analýzy přitom není zjevné, jak je možné tyto požadavky naplnit ani jaký je zdroj těchto požadavků. Vyhodnocení a naplnění těchto požadavků tak povede k velké administrativní zátěži na straně povinných osob. Tuto administrativní zátěž by bylo možné podstatně snížit, pokud by právní úprava vyjasnila, které požadavky jsou již zahrnuty v rámci mezinárodně uznaných certifikací a je možné jejich splnění prokázat prostřednictvím těchto certifikací. Navrhujeme proto stanovit, že tyto požadavky je možné splnit prostřednictvím některé standardní mezinárodní certifikace (jako jsou ISO řady 27xxx) a případně jednoznačně stanovit, které požadavky jsou nad rámec těchto mezinárodních standardů a musejí být tedy naplněny samostatně. K tomu rovněž navrhujeme, aby došlo k detailnímu namapování jednotlivých bezpečnostních požadavků v předkládaných bezpečnostních vyhláškách na existující mezinárodní certifikáty a/nebo stávající vyhlášku č. 82/2018 Sb., o kybernetické bezpečnosti. Takový postup NÚKIB již zvolil např. v rámci legislativního procesu při přijímání tzv. cloudové vyhlášky č. 2 (vyhlášky stanovující obsah a rozsah	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu, včetně bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci ve smyslu § 6 písm. e) zákona č. 181/2014 Sb., o kybernetické bezpečnosti).	
Vyhláška o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností	§ 5 Povinnosti vrcholového vedení	Umožnit outsourcing/pověření výkonem konkrétních povinností nad rámec obecné odpovědnosti za „zajištění“ těchto činností na osobu odlišnou od vrcholového vedení. (pro účely podnikatelských seskupení není praktické, aby tyto povinnosti vykonávali členové vrcholového vedení v každé povinné osobě v rámci seskupení. Zejména se tato připomínka týká o § 5 odst. 1 písm. a), d), f) a g) (v ostatních případech vnímáme, že možnost outsourcingu je již obsažena ve formulaci „zajistí“) a odst. 2.	
Vyhláška o nepominutelných funkcích stanoveného rozsahu Příloha k vyhlášce	Navrhujeme vypuštění tohoto bodu: 1.15 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic.	**Obecné ustanovení** (obecná skutková podstata) nepominutelných funkcí kompletním výčtem ze specifikací 3GPP nezakládá předvídatelnost dané regulace a předpokládaný obsah výroku a odůvodnění OOP, které bude ve věci omezení dodavatele vydáváno. Odůvodnění vyhlášky o nepominutelných funkcích i odůvodnění návrhu zákona se zaměřuje na části jádra sítě (pozn. Core), avšak některé z nepominutelných funkcí mohou být vykládány jako části sítě transportní,	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		popř. RAN – 1.15 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic. Pokud by tento bod byl NÚKIB interpretován jako části RAN případně přenosové sítě, není však důvodné uvalovat regulaci na tyto části sítě, jejichž narušení je velice nepravděpodobné, a navíc by nedošlo k plošnému omezení služby (někdy ani v rozsahu průřezových kritérií v Nařízení vlády 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury) a narušení integrity a dostupnosti služby jako takové, ale pouze k výpadku přenosu signálu, a tím ke krátkodobému výpadku služby pro malou část zákaznické báze v omezeném geografickém území.	
Vyhláška o nepominutelných funkcích stanoveného rozsahu	Navrhujeme zařazení seznamu nepominutelných funkcí do (i) přílohy ZKB, případně vydat takový seznam (ii) formou Nařízení Vlády	Forma vyhlášky pro stanovení nepominutelných funkcí dává NÚKIB extrémně velký prostor pro okamžitou změnu obsahu takového nařízení bez dohledu Vlády ČR anebo Parlamentu ČR a jednání NÚKIBu *ultra vires*. Vyhláška je definována i vydávána právě NÚKIBem, který má bez dohledu a schválení Vlády možnost změny jejího obsahu. NÚKIB tak nejen touto vyhláškou získává možnost omezit obchodní aktivity společností a dodavatelů a současně i jejich odběratelů ze zemí a podle kritérií, které si sám určí, a to za situace, kdy je jediným oprávním prostředkem přezkum OOP soudem.	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
		Takové jednání může navíc vést k rozporu s právem na svobodné podnikání dle Listiny základních práv a svobod. Přijatelnou formou se jeví možnost zařazení seznamu Nepominutelných funkcí (po konkretizaci) do přílohy odděleného ZKB (případně zákona o BDŘ), kdy jejich předloha v 3GPP specifikacích zajistí zároveň aplikovatelnost i na budoucí generace sítí a tím nebude nutná častá aktualizace. Variantním řešením je vydání seznamu Nepominutelných funkcí nařízením vlády, tak, jak je to např. u nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.	
Vyhláška o inspektorech, str. 4	§ 6 Zkouška inspektora 3) Úspěšně vykonaná zkouška má pro potřeby § X odst. 1 [Inspektoři] zákona platnost 1 rok ode dne vykonání.	Znamená to, že proces vypadá tak, že kandidát úspěšně složí zkoušku a má 1 rok na to, aby si zažádal o autorizaci, která mu bude platit 3 roky od schválení? Následně musí před vypršením platnosti autorizace zažádat o prodloužení, které mu NÚKIB schválí nebo ne bez dodatečného přezkoušení apod.? Bude NÚKIB organizovat nějaké školení s ohledem přípravy na zkoušku?	
Vyhláška o inspektorech, str. 6	§ 8 Výběr inspektora Úřadem Úřad se při výběru inspektora podle § X odst. 3 [Kontrola vykonávaná inspektory] zákona řídí vzestupně	Jako to bude fungovat v praxi? Nemůže nastat situace, že inspektoři na začátku seznamu budou mít více kontrol než ti, kteří budou na konci?	

Přesné označení návrhu předpisu a konkrétního ustanovení (název předpisu a paragraf, odstavec, písmeno – pokud neexistují, název ustanovení)	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny** (podrobně rozveďte Váš návrh – důvody, cíle, způsob provedení – Úřad bude z komentáře vycházet při zapracování změn)	**Vypořádání** (vyplní Úřad)
	řazeným abecedním seznamem příjmení inspektorů. Úřad při výběru inspektora zohlední specifické okolnosti případu. Pokud ustanovený inspektor nebude schopen z vážných důvodů kontrolu vykonat, Úřad ustanoví dalšího inspektora v pořadí.		
Vyhláška o inspektorech, str. 6	§ 9 Určení délky trvání kontroly	Chápeme správně, že na začátku se vychází z tabulky v příloze č.2 + dodatečně podle bodů 1) a 2)?	