SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

NÁZEV MATERIÁLU	Připomínky Svazu průmyslu a dopravy České republiky k materiálu Návrh zákona o kybernetické bezpečnosti
Č. J.	57/2023
DATUM ZPRACOVÁNÍ	19. července 2023
KONTAKTNÍ OSOBA	Kateřina Kalužová
TELEFON	225 279 202
E-MAIL	kkaluzova@spcr.cz

Svaz průmyslu a dopravy ČR oceňuje zapracování řady připomínek z veřejné konzultace a významné věcné úpravy návrhu zákona. Nadále ale trváme na tom, aby většina povinností byla ideálně stanovena přímo v zákoně nikoli prostřednictvím prováděcích vyhlášek. Stejně tak trvá výhrada k nedostatečnému definování některých pojmů, u nichž bude přetrvávat aplikační nejistota. Rovněž trvají výhrady k pravidlům hlášení kybernetických bezpečnostních incidentů (§ 16 a násl.). Není totiž zřejmé, zda je možné hlásit pouze významné incidenty nebo zda je nutné hlásit všechny. Lze se tudíž obávat významné administrativní náročnosti při aplikaci navržených pravidel. Metodická podpora NÚKIB bude zcela zásadní.

U neimplementační části zákona týkající se mechanismu prověřování bezpečnosti dodavatelského řetězce zásadní koncepční výhrady přetrvávají, přestože došlo k věcnému posunu oproti verzi zaslané k veřejné konzultaci. Zůstávají například nevyřešené otázky v oblasti řešení vlastnické struktury dotčených dodavatelů, nereflektující zejména existenci soukromoprávních smluvních vztahů mezi poskytovateli regulovaných služeb a dodavateli (včetně možného uplatnění náhrady škod, sankcí atd.

Níže naleznete podrobné připomínky Svazu průmyslu, které jsou pro přehlednost rozděleny do několika sekcí. Veškeré připomínky považujeme za zásadní.

ZÁSADNÍ PŘIPOMÍNKY

I. Přetrvávající zásadní připomínky (byly uplatněny již v rámci veřejné konzultace)

Přesné označení návrhu předpisu a konkrétního ustanovení	**Navrhovaná změna** (popište Vámi navrhované nové řešení, navrhněte finální znění změny)	**Komentář změny a odůvodnění**	**Vypořádání** (vyplní Úřad)
Zákon o kybernetické bezpečnosti *§ 2 Vymezení pojmů, odst. 2 písm f a g* *§ 16 Hlášení kybernetických bezpečnostních incidentů odst. 1 a 2*	Úprava definice ve smyslu vyloučení úmyslného zavinění Např: *kybernetickým bezpečnostním incidentem narušení bezpečnosti informací v rámci aktiv v případě, že nelze vyloučit úmyslné zavinění*	Rozumíme správně, že poskytovatelé v režimu vyšších povinností nemají povinnost hlásit NÚKIB tzv. provozní incidenty, které z povahy věci pod jeho působnost nespadají a incidenty, u kterých lze s jistotou vyloučit úmyslné zavinění a nemají pro vyhodnocování ze strany NÚKIB a další mapování bezpečnostní situace v kybernetickém prostoru zásadnější význam. Takto je i uvedeno v důvodové zprávě. Jak je nyní definováno v § 16, odst. 1, subjekty mají povinnost hlášení incidentů, které vznikly v kyberprostoru. Tato definice i na základě proběhlých jednání vyčleňuje z povinnosti incidenty, které vznikly neúmyslným zaviněním a případnou chybou samotného subjektu, např. při plánovaných pracích. V tomto smyslu hovoří i důvodová zpráva k Zákonu. Bylo by tedy vhodné upravit formulace samotného pojmu „kybernetický bezpečnostní incident“. NCSC definuje kybernetický incident jako porušení bezpečnosti aktiva (systému) s cílem ovlivnit jeho integritu nebo dostupnost nebo neoprávněný přístup nebo pokus o neoprávněný přístup k aktivu (systému) s cílem porušit jeho důvěrnost. Doporučujeme využít Metodiku k hlášení kybernetického bezpečnostního incidentu NÚKIB https://www.nukib.cz/download/publikace/podpurne_materialy/Metodika-hlaseni-incidentu_1.1.pdf, která uvádí:	

		Kybernetický bezpečnostní incident není potřeba NÚKIB hlásit v případě, kdy došlo v důsledku technického selhání k nedostupnosti části aktiv, lze s jistotou vyloučit úmyslné zavinění (zejména útočníkem). Zároveň doporučujeme vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů. *„a zároveň řádné zafungování k nim záložních (redundantních, zdvojených) aktiv zabránilo vzniku nedostupnosti systému jako celku.“* Doporučujeme vyloučit ze současné Metodiky podmínku řádného fungování záložních systémů. Cílem je hlášení incidentů, kde nelze vyloučit úmyslné zavinění bez ohledu na dostupnost.	
Důvodová zpráva Zákona o kybernetické bezpečnosti *§ 17 Náležitosti hlášení kybernetických bezpečnostních incidentů*	V odst. 5 vypustit slova *„nebo svévolným“* z věty *"Prvotní hlášení obsahuje informace o tom, zda existuje podezření, že incident byl způsoben nezákonným ~~nebo svévolným~~ zásahem, a zda je pravděpodobné, že bude mít přeshraniční dopad.“*	Incident, který vznikl svévolným způsobem nenaplňuje podmínky vzniku takového incidentu v kyberprostoru, jak zakládá znění § 16 odst. 1.	

Zákon o bezpečnosti kybernetické *§ 4 Kritéria pro identifikaci regulované služby,* *Vyhláška o regulovaných službách*	Změnit formu prováděcího předpisu na nařízení vlády. V § 4 odstavec 1 nahradit slova „*prováděcí předpis*“ slovy „*vláda nařízením*“. V § 4 odstavec 2 nahradit slova „*Prováděcí předpis*“ slovy „*Vláda nařízením*“.	Původní znění umožňuje NÚKIB, aby na základě vlastního uvážení rozhodoval o okruhu jím regulovaných subjektů, přičemž zákon nevylučuje, aby tento okruh byl rozšířen na libovolný subjekt v rámci vyjmenovaných odvětví. Taková míra koncentrace pravomocí v rukou jednotlivého orgánu veřejné správy je v demokratickém a právním státě nepřijatelná. Navrhovaná změna má za cíl přenést pravomoc určování rozsahu působnosti zákona o kybernetické bezpečnosti na Vládu ČR obdobně jako v případě nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, které v současnosti určuje prvky infrastruktury, na něž dopadá nejpřísnější režim regulace dle zákona o kybernetické bezpečnosti.	
Zákon o kybernetické bezpečnosti *§ 12 Hlášení údajů poskytovatelem regulované služby, odst. 2a a 2c* *Vyhláška o portálu NÚKIB*	Vynechat požadované údaje, které má NÚKIB dostupné v základních registrech (například informace o vlastnické struktuře viz požadavek § 3 Vyhlášky o portálu NUKIB)	Portál NÚKIB by měl být napojen na základní registry, tudíž by registrační a doplňující údaje měly být z velké části, ne-li všechny, z těchto registrů vyčteny.	

Zákon o kybernetické bezpečnosti *§ 19 Informační povinnost poskytovatele regulované služby odst. 1*	Doporučujeme doplnit následovně *„V rozhodnutí o uložení této povinnosti stanoví Úřad rozsah informační povinnosti. **Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby a povinné osoby.***“	Rozsah informační povinnosti není nijak upřesněn/omezen. NÚKIB tak může vyzvat ke zveřejnění informací bez znalosti celkového kontextu incidentu. Přílišná transparentnost může být v některých případech ohrozit bezpečnost regulovaných služeb a kritické infrastruktury.	
Zákon o kybernetické bezpečnosti *§ 21 Výstraha*	Doplnit následující formulaci: *Zveřejnění informace nesmí ohrozit bezpečnost nebo provoz regulované služby.*	Zveřejnění klasifikovaných informací a případného nesouladu s tímto zákonem může vést k narušení bezpečnosti informací a samotného smyslu zákona zajistit bezpečnost regulovaných služeb	
Zákon o kybernetické bezpečnosti *§ 25 Speciální úprava předání informací a dat od významného dodavatele odst. 1.*	Doporučujeme přeformulovat nebo upřesnit spojení „…**hrozícího** kybernetického bezpečnostního incidentu…“.	Z textu zákona není zřejmé, jakou metrikou bude vyhodnocována míra hrozby incidentu, která se nelehko kvantifikuje, pokud takový incident ještě nenastal. Není zřejmé, kdo určí, že se jedná o hrozící incident, a tedy oprávněnost žádosti. Jedná se podle definice o Událost? O jaká data a informace se jedná, pokud incident ještě nenastal? Bez vyjasnění může docházet ke zneužití a nepřesným interpretacím.	

Zákon o kybernetické bezpečnosti *§ 25 Speciální úprava předání informací a dat od významného dodavatele odst. 1*	Za větu „*Úřad může v rozhodnutí určit formát, rozsah, způsob a lhůtu předání a stanovit povinnost po provedení předání tyto informace a data a jejich kopie bezpečně zlikvidovat.*“ doplnit: Formát, rozsah, způsob a lhůta předání informací nesmí jít nad rámec smluvních závazků.	Je nutné respektovat smluvní ujednání.	
Zákon o kybernetické bezpečnosti *§ 28 Prověřování rizik spojených s dodavatelem odst. 1* *Ve spojení s § 29 odst. 3*	Na konec odstavce 1 § 28. doplnit větu „*Úřad využívá data výhradně za účelem vyhodnocování rizikovosti dodavatelů*“.	Původní znění explicitně neomezuje účel sběru informací, účel žádostí ani charakter sbíraných a vyžadovaných informací. Absence těchto omezení vytváří zjevně nezamýšlený prostor pro zneužití institutu sběru údajů a součinnosti k neodůvodněnému shromažďování údajů o právnických i fyzických osobách. Původní znění by bylo možné vykládat např. tak, že zakládá povinnost poskytovatele služeb elektronických komunikací poskytnout NÚKIB na vyžádání shromažďované provozní a lokalizační údaje, ačkoli takové poskytnutí by ve většině případů bylo neproporcionálním zásahem do ústavně chráněného základního práva na soukromí.	
Zákon o kybernetické bezpečnosti, *§ 28 odst. 4* *„… kritéria rizikovosti dodavatele a způsob jejich vyhodnocení stanoví **prováděcí právní předpis.***“	Nevydávat Vyhlášku o kritériích rizikovosti dodavatele a její obsah přenést do zákona o kybernetické bezpečnosti (přílohu vyhlášky, která stanovuje kritéria rizikovosti, doplnit jako přílohu samotného zákona).	Původní znění zakládá právní nejistotu pro poskytovatele strategicky významných služeb i bezpečnostně významné dodavatele, protože kritéria hodnocení rizikovosti se mohou v budoucnu významně a snadno změnit změnou vyhlášky. Původní znění v tomto směru pro obsah vyhlášky nestanoví žádné limity.	

		Ponechání této kompetence v rukou moci výkonné, nikoli zákonodárné, by vedlo k nepřiměřené koncentraci pravomocí v rukou jednoho z orgánů veřejné moci. Nelze přitom akceptovat vypořádání připomínky z veřejné konzultace, dle kterého je úprava kritérií formou podzákonného právního předpisu běžnou legislativní praxí. Podstata hodnocení bezpečnosti dodavatelského řetězce a dostupná opatření se závažností dopadu blíží opatřením podle zákona č. 34/2021 Sb. o prověřování zahraničních investic, přičemž zde jsou základní parametry hodnocení rovněž stanoveny zákonem. Současně již nyní navrhovaná kritéria jsou svou povahou obecná, lze proto očekávat minimum jejich změn. K jejich vyčlenění do prováděcího právního předpisu tedy není racionální důvod. S ohledem na závažný ekonomický i provozní dopad na poskytovatele regulované služby tedy nelze akceptovat model, kdy by kritéria byla stanovena vyhláškou.	
Zákon o kybernetické bezpečnosti, *§ 28 Prověřování rizik spojených s dodavatelem odst. 3 písm. a)* *„…u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního*	Vypustit slova „*vysoká nebo*“.	Poskytovatelé strategicky významných služeb, kteří jsou povinnými osobami podle zákona č. 181/2014 Sb., mají klasifikovaná aktiva a u řady těchto aktiv může být dopad narušení bezpečnosti informací ohodnocen úrovní vysoká, aniž by přitom bylo přiměřené u těchto aktiv aplikovat mechanismus prověřování. Přijetí nového zákona přitom nebude odůvodňovat samo o sobě změnu hodnocení dopadu narušení bezpečnosti informací na tato aktiva. Je proto namístě aplikovat tento mechanismus pouze na aktiva s hodnocením dopadu úrovní kritická. Omezení kritické části stanoveného rozsahu pouze na aktiva s hodnocením dopadu úrovní kritická přitom	

*předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní **vysoká nebo** kritická; …“*		nevytváří riziko nedostatečného zahrnutí klíčových aktiv.	
Zákon o kybernetické bezpečnosti *§ 29 odst. 1 a 2*	Mezi orgány, které mají poskytovat Úřadu informace a součinnost, doplnit Český telekomunikační úřad (ČTÚ).	Návrh zákona o kybernetické bezpečnosti a související předpisy významně dopadají na poskytovatele regulovaných služeb v oblasti služeb elektronických komunikací, přesto původní znění výslovně nezmiňuje mezi orgány poskytujícími součinnost ČTÚ (jakkoli jej lze považovat za „orgán“ podle odst. 3). ČTÚ má přitom ve vztahu k oblasti služeb elektronických komunikací největší odbornost, dohlíží nad bezpečností a integritou komunikačních sítí a ukládá opatření k řešení hrozeb (§ 98 zákona č. 127/2005 Sb., o elektronických komunikacích), díky čemuž disponuje řadou informací významných z hlediska technologií, které je pro zajištění bezpečnosti dodavatelského řetězce třeba zohlednit (zejména z hlediska nepominutelných funkcí stanoveného rozsahu).	
Zákon o kybernetické bezpečnosti *§ 29 odst. 3*	Vypustit odst. 3	Původní znění explicitně neomezuje okruh dalších orgánů a osob, které jsou povinny poskytnout Úřadu informace a součinnost. To vytváří potenciál k zatížení povinných osob mechanismu prověřování dodatečnými povinnostmi k poskytování údajů, typicky v reakci na hlášení podle § 32 odst. 1 písm. b), a tak faktické rozšiřování výčtu údajů podle § 4 odst. 4 Vyhlášky o portálu NÚKIB.	

		Okruh osob a orgánů povinných k součinnosti vůči NÚKIB v této oblasti by měl být stanoven taxativně.	
Zákon o kybernetické bezpečnosti, *§ 29 Prověřování rizik spojených* *s dodavatelem odst. 3 písm. c)* *„… dodavatelem bezpečnostně významné dodávky každý, kdo poskytovateli strategicky významné služby poskytne přímo* ***či jako poddodavatel*** *bezpečnostně významnou dodávku.“* *Ve spojení s § 32 odst. 1 písm. a)* *„… zjišťovat s vynaložením* ***přiměřeného úsilí*** *informace* *o dodavatelích bezpečnostně*	Doplnit úroveň poddodavatelského řetězce, která má být předmětem zjišťování povinné osoby mechanismu prověřování dle § 32 odst. 1 písm. a), nebo způsoby pro její stanovení (např. odkaz na prováděcí právní předpis a zmocnění k jeho vydání).	Je třeba blíže specifikovat úroveň dodavatelského řetězce, do které jsou poskytovatelé strategicky významných služeb povinni zjišťovat informace dle § 32 odst. 1 písm. a). V souladu s cílem a účelem předmětné úpravy je přiměřené, aby poskytovatel strategicky významné služby zjišťoval informace nejen o primárním dodavateli, kterým bude často pouze distributor, ale také o přímém výrobci daného produktu nebo poskytovateli služby ve vztahu, ke kterým je stěžejní prověřit rizikovost. Původní znění však lze vykládat i jako povinnost zjišťovat informace i o dodavatelích jednotlivých komponent daného výrobku (polovodičových prvků) nebo dodavatelích dílčích programových prostředků (licencí), pomocí kterých je poskytována služba přímým dodavatelem. Taková povinnost pro poskytovatele strategicky významných služeb by byla nepřiměřená a není opodstatněna bezpečnostními riziky, která jednotlivé komponenty či programové vybavení představují pro kybernetickou bezpečnost regulované služby. Tato hloubka prověřování by naopak byla přiměřená v případě služeb elektronických komunikací, kde by poskytovatelé strategicky významných služeb měli zjišťovat informace o dodavatelích použité infrastruktury, jakožto bezpečnostně významných dodavatelích, přičemž by měli promítnout opatření obecné povahy spočívající v zákazu nebo stanovení	

významných dodávek a…“		podmínek využívání plnění bezpečnostně významného dodavatele i na dodavatele infrastruktury pro využívané služby elektronických komunikací. Vypořádání připomínky z veřejné konzultace nevyrovnává s různorodou povahou poddodavatelů popsanou výše (dodavatelé software vs. komponent). Ze skutečnosti, že hloubka prověřování musí být přiměřená, neplyne možnost některé dodavatele, kteří nemají význam z hlediska kybernetické bezpečnosti, zcela ignorovat.	
Vyhláška o nepominutelných funkcích stanoveného rozsahu, *bod 1.11 a 1.14 přílohy* *„1.11 Systémy řízení veřejné komunikační sítě a monitorování této sítě, včetně řízení a monitoringu kybernetické bezpečnosti, pokud se tyto systémy týkají řízení nebo monitorování nepominutelných funkcí veřejné komunikační sítě nebo pokud mohou mít významný dopad na*	Vypustit body 1.11 a 1.14	Uvedené typy aktiv nepovažujeme za nezbytné pro zajištění fungování jádra sítě elektronických komunikací, a proto by neměly tvoři součást nepominutelných funkcí stanoveného rozsahu.	

přístup k síti nebo na síťový provoz.“ *„1.14 Funkce řízení rádiové přístupové sítě 2., 4. a 5. generace a řízení základnových stanic.“*			
Zákon o kybernetické bezpečnosti, *§ 30 Omezení rizik spojených s dodavatelem*	Za odstavec 3 vložit nový odstavec 4 ve znění „Ukládá-li opatření obecné povahy povinnost poskytovateli služeb elektronických komunikací, má Český telekomunikační úřad v řízení o vydání opatření obecné povahy postavení dotčeného orgánu. Dotčený orgán uplatňuje v řízení stanoviska, která nejsou rozhodnutím ve správním řízení a jejichž obsah je závazný pro vydání opatření obecné povahy podle odst. 1.“	ČTÚ disponuje nejširší expertízou v oblasti trhu služeb elektronických komunikací a dohlíží nad bezpečností a integritou veřejných komunikačních sítí a služeb elektronických komunikací. Závažné zásahy do trhu poskytování služeb elektronických komunikací nelze efektivně provádět bez informací, jimiž disponuje pouze sektorový regulátor, který je ze zákona eviduje a zpracovává. ČTÚ ze zákona náleží dohled nad trhem se službami elektronických komunikací, který nelze účinně provádět, bude-li do trhu zasahovat jiný správní orgán bez nutnosti vyžádání stanoviska, potenciálně i bez vědomí ČTÚ. Současně musí mít sektorový regulátor k dispozici informace o připravovaných zásadních zásazích do jím regulovaného trhu. Spolupráce s dotčeným orgánem také snižuje zátěž povinných osob z hlediska poskytování obdobné součinnosti jak NÚKIB, tak ČTÚ. Návrh má za cíl vytvořit obdobný mechanismus stanovisek dotčeného orgánu k mechanismu stanovisek dotčených orgánů podle § 54 zákona č. 283/2021 Sb.,	

		stavebního zákon (a obdobně podle zákona č. 183/2006 Sb.), přičemž kromě ČTÚ by dotčenými orgány mohli být také ostatní sektorový regulátoři (např. ERÚ, ÚCL apod.). Takový mechanismus zároveň sníží koncentraci pravomocí NÚKIB, který má v původní podobě návrhu možnost významně zasáhnout do téměř všech odvětví národního hospodářství bez ohledu na existenci a stanovisko regulační autority příslušného sektoru. Vypořádání připomínky z veřejné konzultace nepovažujeme za dostatečné. Argumenty vznesené ve vztahu k NÚKIB lze analogicky uvést i u obce či kraje jako pořizovatelů územně plánovací dokumentace, přesto jsou obec i kraj při pořizování územně plánovací dokumentace vázány stanovisky dotčených orgánů a nadřízeného orgánu.	
Zákon o kybernetické bezpečnosti, § 32 Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 1 písm. a) a b) *„… zjišťovat s vynaložením přiměřeného úsilí informace o dodavatelích bezpečnostně významných dodávek*	Upřesnit, že bezpečnostně významnou dodávkou plynoucí z rámcové smlouvy je uzavření rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb jako celku (se specifikací rozsahu rámcové smlouvy), nikoli jednotlivé dílčí plnění (objednávky).	V případě, že by každé jednotlivé dílčí plnění (realizovaná objednávka) z rámcové smlouvy na dodávku určitého výrobku nebo služby, popř. skupiny výrobků nebo služeb, mělo být hlášeno jako samostatná bezpečnostně významná dodávka, byla by na poskytovatele strategicky významné služby kladena neúměrně vysoká administrativní zátěž a stejně tak NÚKIB by byl zatížen řadou nadbytečných hlášení bez přidané informační hodnoty. Účel tohoto ustanovení bude naplněn i ve znění navrhované změny, dle které se plnění plynoucí z rámcové smlouvy budou hlásit jako jedna bezpečnostně významná dodávka s určením možného rozsahu plnění. Vypořádání připomínky z veřejné konzultace nereflektuje že návrh se vztahuje k opakovanému	

*a dokumentovat tyto informace alespoň v rozsahu **identifikace všech bezpečnostně významných dodávek** a dodavatelů bezpečnostně významných dodávek, kteří je poskytují,“*		objednávání stejného plnění (zboží) tedy nezměněného bezpečnostního rizika.	
Zákon o kybernetické bezpečnosti, *§ 32 Povinnosti spojené s prověřováním bezpečnosti dodavatelského řetězce odst. 2* *„Poskytovatel strategicky významné služby začne **plnit povinnost hlásit informace podle odstavce 1** pro každou strategicky významnou službu **nejpozději do 1 roku ode dne doručení písemného vyrozumění o jejím zápisu do evidence***	Doplnit, že doba 1 roku ode dne doručení písemného vyrozumění o zápisu se vztahuje také na povinnost zjišťovat informace podle § 32 odst. 1 písm. a).	Přechodné období by se nemělo uplatnit pouze pro povinnost hlásit NÚKIB informace, ale i pro povinnost je zjišťovat. Není přiměřené požadovat, aby poskytovatelé strategicky významných služeb zahájili sběr informací bezprostředně po účinnosti zákona, bez stanovení přechodného období. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že plnění povinnosti zjišťovat informace nelze zahájit okamžitě. K okamžiku zápisu do evidence poskytovatelů regulované služby nebude mít poskytovatel strategicky významné služby nastaveny odpovídající smluvní a compliance mechanismy a v případě kontroly bezprostředně po tomto zápisu bude čelit riziku významných sankcí ze strany NÚKIB. I proto povinnost je tak třeba nastavit odložené plnění, aby bylo možné zavést příslušné smluvní a compliance mechanismy.	

poskytovatelů regulovaných služeb *podle § 10 odst. 1.“*			
Zákon o kybernetické bezpečnosti, *§ 33 Omezení rizik spojených s dodavatelem ve veřejných zakázkách*	Odstranit z § 32 slova *„v postavení zadavatele podle právního předpisu upravujícího zadávání veřejných zakázek“* a slova *„na veřejnou zakázku“.*	I soukromý subjekt, který není zadavatelem podle zákona o zadávání veřejných zakázek, může mít sjednaný dlouhodobý závazek, při jehož sjednávání nemohl vědět, že jeho dodavatel bude shledán rizikovým dodavatelem. Řada takových závazků může být sjednána před účinností navrhovaného zákona. Pro takové případy je třeba stanovit mechanismy umožňující i takovému soukromému subjektu ukončit sjednaný závazek. Vypořádání připomínky z veřejné konzultace nereflektuje skutečnost, že některé kontrakty na bezpečnostně významné dodávky jsou dlouhodobé a mohly být sjednány před přijetím navrhované právní úpravy a tedy ji nemohly předvídat a nemusí v ní být obsažen adekvátní výpovědní důvod.	
Zákon o kybernetické bezpečnosti *§ 40 Opatření k řešení stavu kybernetického nebezpečí odst. 1 g)*	Vypustit	Zákon nedefinuje rozsah ani metodiku provedení skenu zranitelností a penetračního testu. Sken zranitelností a penetrační test technických aktiv provedený na jejich produkční části může zásadně narušit funkčnost technických aktiv až do míry ekvivalentní reálnému kybernetickému útoku, může způsobit nestabilitu, dlouhodobé selhání, případně přímo usnadnit budoucí kybernetický útok. Provedení skenu zranitelností a penetračního testu musí být vždy v odpovědnosti vlastníka nebo provozovatele technických aktiv a musí být prováděno v rámci plánovaných výlukových oken, a to v definovaném rozsahu s odhadnutelným dopadem.	

Zákon o kybernetické bezpečnosti *§ 53 Zpracování osobních údajů odst. 1*	Vypustit slovo *„úkolů“* a přidat slovo *„oprávněným“* z/do věty *„Tyto údaje Úřad a provozovatel Národního CERT předávají **oprávněným** orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich ~~úkolů~~ zákonných povinností a nedojde-li tím k porušení povinnosti mlčenlivosti podle tohoto zákona.“*	Zajistit soulad s účinnými právními normami, jako je GDPR, která specifikují pravomoci a zmocnění oprávněných orgánů při plnění jejich zákonných povinností.	
Zákon o kybernetické bezpečnosti *§ 53 Zpracování osobních údajů odst. 3 a), 3 b), 3 c)*	Doplnit soulad s GDPR a dalšími právními předpisy	V případě, kdy mají být subjektům údajů odepřena jejich práva, je nutné zákonem vymezit konkrétní účely a podmínky zpracování osobních údajů, a to včetně retenčních povinností. Současně je nutno zakotvit zákonný mechanismus kontroly oprávněnosti a zpracování takovýchto osobních údajů.	

II. Připomínky BDŘ a lokalizace

Zákon o kybernetické bezpečnosti, *§ 28 Prověřování rizik spojených s dodavatelem* *odst. 3 písm. a)* *„… aktiva stanoveného rozsahu strategicky významné služby,* ***která zajišťují nepominutelné funkce stanoveného rozsahu stanovené***	písm. a) Vypustit „*která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem*“ a nahradit „*úrovní kritická; a jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby*,“ písm. c) Vypustit *„či jako poddodavatel.“*	Navrhované ustanovení ponechává pravomoc NÚKIB provádět prověřování rizik spojených s dodavatelem, tak jak přepokládá návrh ZKB, odlišně však vymezuje některé pojmy spojené s touto pravomocí. Vzhledem k odlišné koncepci pojmu kritické části stanoveného rozsahu (viz níže), je obsolentní zakotvení vydání vyhlášky o nepominutelných funkcích stanoveného rozsahu, jak předpokládá návrh ZKB, proto byla ze znění tohoto návrhu vypuštěna. Pravomoc NÚKIB má být realizována, v souladu s návrhem ZKB, prostřednictvím shromažďování a vyhodnocování informací, jež mohou přispět k vyvození závěrů o existenci hrozby pro bezpečnost ČR, vnitřní či veřejný pořádek nebo naplnění kritérií rizikovosti dodavatele stanovených prováděcím právním předpisem, a které jsou spojeny s plněním konkrétního	

***prováděcím právním předpisem**,“* *odst. 3 písm. c)* *c) dodavatelem bezpečnostně významné dodávky ten, kdo poskytovateli strategicky významné služby poskytne přímo či jako **poddodavatel** bezpečnostně významnou dodávku.*		dodavatele. Kritéria rizikovosti dodavatele stanoví prováděcí právní předpis – vyhláška, k jejímuž vydání je zmocněn NÚKIB v § 55 návrhu ZKB. Jak je uvedeno v důvodové zprávě k návrhu ZKB, cílem mechanismu prověřování BDŘ je umožnit státu identifikovat a vyhodnocovat hrozby spojené jak s orgány nebo osobami, které již jsou dodavateli do infrastruktury poskytovatelů strategicky významné služby, tak s orgány nebo osobami, u nichž se lze domnívat, že by svá plnění do této infrastruktury dodávat mohly, a to s cílem odhalit hrozbu ještě dříve, než bude u strategicky významné služby moci způsobit narušení bezpečnosti informací. S ohledem na velké množství orgánů a osob, které mohou být předmětem prověřování, je stanovena možnost NÚKIB prioritizovat činnosti spojené s prověřováním stávajících a potenciálních dodavatelů, tak jak to předpokládá i návrh ZKB, a to s ohledem na možná rizika a dostupné kapacity NÚKIB. Odst. 3 předmětného ustanovení vymezuje pojmy, které navrhovaná právní úprava dále užívá v souvislosti s mechanismem. Pojem „bezpečnostně významná dodávka“, který vymezuje plnění, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů, a „dodavatel bezpečnostně významné dodávky“, který vymezuje okruh orgánů a osob, na jejichž plnění se mohou vztahovat omezení využití v důsledku prověření rizik s nimi spojených, je dle tohoto návrhu shodný se zněním uvedeným v návrhu ZKB, proto se mu text zde nebude věnovat. Změny však v tomto předkládaném návrhu doznal pojem „kritická část stanoveného rozsahu“, který vymezuje aktiva poskytovatele strategicky významné	

		služby, na která se mohou vztahovat omezení využití plnění rizikových dodavatelů. NÚKIB opakovaně deklaroval, že mechanismus se má vztahovat pouze na tu nejkritičtější část strategické infrastruktury. V návrhu ZKB je však vymezen rozsah mechanismu formou vyhlášky o nepominutelných funkcí, která je výrazně širší než bylo deklarováno, a např. pro oblast telekomunikací obsahuje jak ty nejkritičtější části sítě (jako je jádro sítě – „core“), tak i méně kritické části sítě (jako je např. rádiová přístupová síť) nebo aktiva, které nemají přímý vliv na nedostupnost regulovaných služeb (např. fakturační systém). V návrhu ZKB i důvodové zprávě k němu zcela chybí odůvodnění, proč jsou kritické části stanoveného rozsahu aktiv definovány tak široce. Ve zde předkládaném návrhu je stanovena nová úprava kritické části stanoveného rozsahu aktiv tak, aby se jednalo pouze o aktiva ohodnocená povinnými subjekty na úrovni kritická, jejichž nedostupnost má současně přímý okamžitý dopad na nedostupnost strategicky významné služby. Předkládaný návrh vychází z předpokladu, že kritická část stanoveného rozsahu se skládá z podmnožiny aktiv strategicky významných služeb, u kterých si poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu upravujícího bezpečnostní opatření poskytovatele regulované služby v režimu vyšších povinností sám v rámci plnění povinností podle § 13 návrhu ZKB ohodnotil dopad narušení bezpečnosti informací úrovní kritická. Kritické části strategické infrastruktury jsou transparentně rozděleny dle úrovně hrozby a dopadů	

		její případné realizace. Nejvýznamnější hrozbou je výpadek regulované služby – rozsah mechanismu tak byl v návrhu omezen výlučně na aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro příklad – pro oblast telekomunikací se jedná zejména o jádro sítě, případně části přenosové sítě. Úprava je formulována obecněji, aby se vztahovala na všechny oblasti, nejen telekomunikace. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je přiměřené, aby byla dána možnost státu okamžitým zásahem omezit či zakázat vybraného dodavatele, u kterého identifkuje významnou hrozbu. Pro zbylé části aktiv strategicky významné služby, které nemohou ze své podstaty způsobit nedostupnost služby na kritické úrovni, je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval NÚKIB. Ten by přitom jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Úpravou písm. c) se tento mechanismus omezí pouze na přímé dodavatele povinných osob, a nikoliv i dalších nepřímých poddodavatelů. Tímto zúžením počtu subjektů, na něž bude dopadat předmětná úprava, dojde k omezení této zásadní administrativní zátěže. Zároveň se předejde situaci, kdy např. povinnosti z předmětné úpravy budou muset plnit také dodavatelé poddodavatelů apod.	

Zákon o kybernetické bezpečnosti, *§ 30 Omezení rizik spojených s dodavatelem*	Navrhujeme nové znění § 30 ve znění: 1. Zjistí-li Úřad na základě vyhodnocení kritérií rizikovosti dodavatele možné významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, předloží věc k projednání Vládě České republiky (dále jen "Vláda"). 2. Vláda přijme do 45 dnů ode dne, kdy jí byla věc předložena k projednání, usnesení o tom, zda plnění dodavatele může představovat ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Při posuzování věci Vláda zohlední možný dopad plnění dodavatele na principy demokratického právního státu, ochranu života a zdraví obyvatel, obranu státu, zahraničně politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. 3. V návaznosti na usnesení Vlády, že plnění dodavatele představuje významné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku, vydá Úřad opatření obecné povahy, kterým stanoví podmínky nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu. 4. Usnesení Vlády je pro Úřad závazné a vydání opatření obecné povahy omezující či zakazující plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu je vydáním usnesení Vlády podmíněno. 5. Zakáže-li nebo omezí-li Úřad opatřením obecné povahy dle odstavce 3 plnění dodavatele, určí zároveň v opatření obecné povahy přiměřenou lhůtu	Jak je uvedeno ve zprávě o hodnocení dopadů, cílem prověřování rizik spojených s dodavatelem je minimalizace ekonomických dopadů a omezení pouze na kritickou část síťové infrastruktury. Pokud je cílem vymezit pouze kritickou část strategické infrastruktury, mělo by se jednat o aktiva, jejichž nedostupnost má přímý okamžitý dopad na nedostupnost regulované služby na kritické úrovni. Pro tyto kritické části, které mohou způsobit okamžitou nedostupnost strategicky významné služby, je tedy vhodné, aby byla možnost státu okamžitým zásahem zakázat vybraného dodavatele, u kterého identifkuje významné hrozby. Pro zbylé části aktiv strategicky významné služby je s ohledem na princip proporcionality vhodné, aby poskytovatel strategicky významné služby sám na základě analýzy rizik minimalizoval rizika, která v rámci opatření obecné povahy identifikoval regulátor. Regulátor by jako doposud nad implementovanými bezpečnostními opatřeními vykonával dohled. Bezpečnostní opatření specifická pro daného dodavatele by nově byla upravena zvlášť v bezpečnostní dokumentaci, kterou by poskytovatel měl povinnost ročně aktualizovat. Nově je navrženo zapojení Vlády ČR do procesu vydávání OOP. Je nezbytné, aby v případě vyhodnocování hrozeb měla Vláda možnost posoudit dopady úkonů Úřadu na principy demokratického právního státu, ochranu života a zdraví obyvatel, obrany státu, zahraničně-politické nebo bezpečnostní zájmy státu, ekonomickou bezpečnost státu a případně další	

	zákazu nebo zohlednění podmínek plnění dodavatele. Lhůtu pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy stanoví Úřad s přihlédnutím k jejich dopadům na poskytovatele strategicky významné služby. Úřad vždy musí lhůtu předem konzultovat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele. 6. Před vydáním opatření obecné povahy je Úřad povinen projednat s příslušnými ústředními orgány státní správy, do jejichž působnosti spadá strategicky významná služba, do které směřuje bezpečnostně významné plnění dodavatele, zda návrh opatření obecné povahy a jeho možné dopady neohrozí plnění povinností stanovených a vyplývajících ze zvláštních právních předpisů. Úřad je povinen při vydání opatření obecné povahy stanovisko ústředního orgánu státní správy zohlednit. 7. Jestliže zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle odstavce 3 může ohrozit poskytování strategicky významné služby anebo představuje bezprostřední hrozbu kybernetického bezpečnostního incidentu, který podstatným způsobem ohrožuje poskytování strategicky významné služby, je poskytovatel strategicky významné služby povinen plnit opatření obecné povahy až po pominutí takové hrozby. 8. Úřad doručí návrh opatření obecné povahy veřejnou vyhláškou a vyzve dodavatele, vůči jehož plnění opatření obecné povahy míří, a další dotčené osoby, aby k návrhu opatření obecné povahy podávali připomínky. Lhůta pro podání připomínek činí 30 dnů,	skutečnosti důležité z hlediska ochrany bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Lhůta plnění povinností poskytovatele z OOP navrhuje stanovovat na základě délky životního cyklu aktiv bezpečnostně významné dodávky, které jsou vyjádřeny účetními odpisy jednotlivých aktiv. V případě, že je taková lhůta zkrácena, znalec stanoví výši náhrady.	

	nestanoví-li Úřad jinak. Ustanovení § 172 odst. 1 a 5, § 173 odst. 1 věty první, část věty za středníkem, a § 173 odst. 1 věty druhé správního řádu se pro postup podle tohoto ustanovení nepoužijí. 9. V případě vydání opatření obecné povahy odstavce 3 musí poskytovatel strategicky významné služby provést analýzu rizik spojených s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3 pro aktiva strategicky významné služby, která nezařadil do kritické části stanoveného rozsahu podle § 28 odst. 3 písm. a). 10. Na základě analýzy rizik vypracuje poskytovatel strategicky významné služby plán zvládání rizik dle odstavce 9, v němž uvede bezpečnostní opatření minimalizující rizika spojená s dodavatelem uvedeným v opatření obecné povahy podle odstavce 3. Plán zvládání rizik je poskytovatel strategicky významné služby povinen aktualizovat alespoň jednou za kalendářní rok. 11. Úřad přezkoumá alespoň jednou za 3 roky trvání skutečností, na jejichž základě bylo vydáno opatření obecné povahy podle odstavce 3. Zjistí-li Úřad, že tyto skutečnosti pominuly, opatření obecné povahy zruší. A nový § 31 ve znění: **§31** **Náhrada účelně vynaložených nákladů** 1. V případě, že lhůta pro zohlednění podmínek nebo zákazu obsaženého v opatření obecné povahy podle §30 odstavce 3 je kratší, než životní cyklus bezpečnostně významné dodávky, nejdéle však 7 let, má každý poskytovatel strategicky významné služby vůči státu právo na náhradu účelně vynaložených nákladů vzniklých v důsledku plnění povinností podle		

	odstavce 3 a to včetně nákladů na náhradu dlouhodobého majetku, který poskytovatel strategicky významné služby v důsledku opatření obecné povahy podle odstavce 3 nemůže dále využívat. Výši účelně vynaložených nákladů podle věty první určí Úřad na základě znaleckého posudku, pro jehož vyhotovení poskytne poskytovatel strategicky významné služby součinnost. 2. Životní cyklus bezpečnostně relevantní dodávky bude znalcem určen na základě účetních odpisů zařízení. 3. Zrušením opatření obecné povahy podle odstavce 11 nezaniká právo na náhradu nákladů podle tohoto odstavce. Ve věci náhrady nákladů podle tohoto odstavce jménem státu jedná Úřad.		
Zákon o kybernetické bezpečnosti, *Aktuální § 31 Výjimky z omezení rizik spojených s dodavatelem* *Nový odst.5*	Doplnit nový odstavec *„(5) Informace týkající se výjimky je v souladu s právními předpisy[1)] označována jako utajovaná informace.“* [1)] *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.*	Udělované výjimky jsou citlivou informací, která může poskytovatele regulované služby významně ohrozit. Domníváme se, že je vhodné klasifikovat informace o procesu udělení výjimky i obsah samotné výjimky, zahrnující subjekty, jichž se výjimka týká jako tajné.	
Zákon o kybernetické bezpečnosti *§ 34 Zajištění dostupnosti*	Navrhujeme: - úpravu odst. 1, 2 a 4, jednak úpravu směřující k vypuštění referencí na případná aktiva směřující k vyjasnění, že dostupnost služby musí být zajištěna v omezeném a pouze nezbytném rozsahu. Pojem „nezbytný“ rozsah, čas a kvalita považujeme za vhodnější, než pojem „stanovený“. Zároveň navrhujeme odkázat na „rozsah“, protože pro některé	Ustanovení § 34 návrhu zákona stanoví povinnosti na zajištění dostupnosti strategicky významných služeb z území České republiky. Pro veřejnou správu je strategicky významná služba definovaná jako „výkon svěřených pravomocí“ ze strany vymezených orgánů státní správy a samosprávy. Vymezený okruh orgánů je	

strategicky významné služby *Využívání cloudových a dalších inovativních služeb*	agendy orgánů veřejné správy nebo jejich části nemusí být nezbytné zajistit dostupnost vůbec. Odkaz na kvalitu a čas implikuje, že je nutné zajistit dostupnost všech agend, bez ohledu na jejich strategický význam, byť případně v omezené kvalitě. - vyjasnění vztahu mezi informačními systémy veřejné správy a požadavky na dostupnost služby, kde zároveň navrhujeme omezení aplikovatelnosti požadavku dostupnosti na informační systémy veřejné správy v bezpečnostní úrovni 4 (kritická). Alternativně by rovněž bylo možné zvažovat úplné vyloučení aplikaci požadavku dostupnosti z území České republiky na veřejnou správu, protože informační systémy veřejné správy v bezpečností úrovni 4 mohou být poskytovány výhradně ve státním cloudu umístěném na území České republiky a požadavek zajištění dostupnosti z území České republiky je pro ně tudíž zjevně nadbytečný. Požadavek dostupnosti z území České republiky by se pak uplatnil pouze na ostatní strategicky významné služby v sektoru energetiky, dopravy a digitální infrastruktury. **<u>Navrhovaná úprava:</u>** **§ 34** (1) Poskytovatel strategicky významné služby je povinen zajistit dostupnost strategicky významné služby ~~v rozsahu kritické části stanoveného rozsahu ve stanoveném~~ **<u>nezbytném</u>** <u>case</u>**<u>,</u>** ~~a~~ kvalitě **<u>a rozsahu</u>** <u>z území České republiky.</u>	velmi široký a zahrnuje, mimo jiné, všechny ústřední orgány státní správy, správní úřady s celostátní působností, kraje, větší obce s rozšířenou působností, vysoké školy, orgány soudní moci a policejní útvary a dalších orgány (dále označovány také jako „orgány veřejné moci“). Dostupnost na území České republiky musí být podle navrhované právní úpravy zajištěna pro všechna aktiva, u kterých by narušení bezpečnosti informací mělo kritický a vysoký dopad na výkon kterékoli agendy svěřené těmto orgánům1. Tato povinnost by se tak v praxi vztahovala na převážnou většinu informačních systémů v české státní správě a samosprávě. Ačkoliv hlavním cílem nového zákona o kybernetické bezpečnosti má být implementace směrnice NIS 2, požadavek na zajištění dostupnosti služeb z území České republiky nemá ve směrnici žádnou oporu a jde nad rámec její implementace do českého právního řádu. Lze i dovozovat, že tento požadavek může být v rozporu s přeshraniční spoluprací v rámci Evropské unie, kdy elektronizace některých agend veřejné správy probíhá ve vzájemné koordinaci jednotlivých zemí. Zdá se, že se jedná o požadavek, které nebyl v navrhované podobě zatím implementován v žádném jiném členském státě EU.	

[1] Definice dotčených aktiv je v navrhovaném textu zákona o kybernetické bezpečnosti v § 28 odst. 3 písm. a) částečně nejasná, nicméně NUKIB předběžně potvrdil výše popsaný výklad. Definice dotčených aktiv dle navrhované právní úpravy je následující (s tím, že „strategicky významnou službou“ je ve státní správě *„výkon svěřených pravomocí“*: *„kritickou částí stanoveného rozsahu aktiva stanoveného rozsahu strategicky významné služby, u kterých poskytovatel strategicky významné služby postupem podle prováděcího právního předpisu ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah strategicky významné služby úrovní vysoká nebo kritická; kritickou částí stanoveného rozsahu jsou vždy alespoň aktiva stanoveného rozsahu strategicky významné služby, která zajišťují nepominutelné funkce stanoveného rozsahu stanovené prováděcím právním předpisem“,*

	(2) Poskytovatel strategicky významné služby je povinen testovat schopnost zajištění poskytování strategicky významné služby ~~v rozsahu kritické části stanoveného rozsahu~~ z území České republiky nejméně jednou za dva roky. (3) Poskytovatel strategicky významné služby začne plnit povinnosti uvedené v odst. 1 a 2 pro každou strategicky významnou službu nejpozději do jednoho roku ode dne doručení vyrozumění o zápisu strategicky významné služby do evidence poskytovatelů regulovaných služeb nebo od doručení rozhodnutí o určení strategicky významné služby podle § 27 odst. 2. (4) ~~Stanovený~~ **Nezbytný** čas~~,~~ ~~a~~ kvalitu **a rozsah** služby stanoví poskytovatel regulované služby v závislosti na cílech řízení kontinuity činností podle prováděcího právní předpisu. (5) Pro potřeby tohoto ustanovení je kritická část stanoveného rozsahu vymezena v § 28 odst. 3 písm. a). **(6) Pokud je pro strategicky významnou službu orgánu veřejné správy využíván informační systém veřejné správy[1], pro který je využíván cloud computing, musí být dostupnost takového informačního systému státní správy na území České republiky pro účely zajištění dostupnosti strategicky významné služby dle odst. 1 zajištěna pouze pro informační systémy veřejné správy zařazené do nejvyšší bezpečnostní úrovně.**	Z praktického hlediska to znamená, že orgány veřejné moci by musely mít zajištěnou dostupnost veškerých informačních systémů používaných pro výkon svých agend z území České republiky. Pro tyto informační systémy by tak musela existovat záložní varianta, která by byla za všech okolností dostupná výhradně z území České republiky (dle výkladu NÚKIB se musí jednat o variantu, která umožní výkon svěřených pravomocí výhradně s využitím aktiv umístěných na území České republiky a nelze ji zajistit např. dvěma zahraničními poskytovateli či privátním připojením). Tyto požadavky mají zásadní dopad na možnost využívání cloudových služeb v české veřejné správě. Orgány veřejné moci by při využití globálních cloudových služeb musely vytvářet paralelní infrastrukturu na území České republiky (tj. zajistit veškerá aktiva paralelně i na území České republiky, tak aby výkon jejich agend byl možný jen s využitím těchto aktiv). To by vedlo k extrémnímu navýšení nákladů na informační systémy. Tato paralelní infrastruktura by musela být trvale udržována, aktualizována, testována a zabezpečena. Pro některé komplexní SaaS a PaaS služby nemusí být zajištění řešení dostupného výhradně z území České republiky vůbec reálné a tyto služby by tak v české veřejné správě nemohly být vůbec využívány. Tento požadavek by velmi pravděpodobně znemožnil využívání zejména vysoce inovativních služeb s prvky umělé inteligence, které není reálné zajistit výhradně z území České republiky, a to ani s vynaložením vysokých nákladů.	

[1] Ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.

		Požadavek na zajištění dostupnosti služeb (z lokálního území) považujeme za opodstatnitelný pro nejkritičtější infrastrukturu státu. Pro veřejnou správu byla tato nejkritičtější informační infrastruktura státu již vymezena prostřednictvím bezpečnostních úrovní (bezpečnostní úroveň 4 – kritická) ve smyslu vyhlášky č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci (která má být nově vydaná ve stejném znění na základě nově předvídaného zmocnění v zákoně č. 365/2000 Sb., o informačních systémech veřejné správy). Pro tyto systémy je již v souladu s § 6m odst. 2 zákona č. 365/2000 Sb., o informačních systémech veřejné správy, možné využívat cloudové služby pouze, pokud jsou poskytovány státním poskytovatelem cloud computingu (tj. je zajištěna dostupnost i poskytování z území České republiky). Rozšiřování těchto povinností na jakékoliv další systémy veřejné správy tak popírá smysl této úpravy a je nepřiměřené. Dopady takového rozšíření by zahrnovaly několikanásobné navýšení nákladů na informační systémy veřejné správy a výrazné zpomalení rozvoje služeb eGovernmentu a digitalizace státní správy.	
Zákon o kybernetické bezpečnosti *§ 34 Zajištění dostupnosti strategicky významné služby*	Mezi aktuální odst. 1 a 2 přidat nový odst. 2. Následující odstavce přečíslovat *„(2) Poskytovatel strategicky významné služby v odvětví 16.1 Poskytování veřejně dostupní služby elektronických komunikací a 16.2. Zajišťování veřejně dostupné komunikační sítě elektronických komunikací podle přílohy Vyhlášky o regulovaných službách je povinen zajistit dostupnost strategicky významné služby uvedené v odst. 2 písm. a) až c),*	NÚKIB na základě připomínek veřejnosti upustil od požadavků na lokalizaci dat na území České republiky nebo spřátelených států. Zároveň však navrhl nahradit lokalizaci povinností zajistit dostupnost strategicky významných služeb z České republiky, pokud jsou k jejich poskytování využívána zahraniční aktiva. Povinnost má zajistit dostupnost nejkritičtějších služeb pro občany České republiky v případě mimořádných	

Služby elektronických komunikací	*v rozsahu kritické části stanoveného rozsahu ve stanoveném čase a kvalitě z území České republiky.* *a) poskytování veřejně dostupné mobilní služby elektronických komunikací* *b) zajišťování veřejné mobilní komunikační sítě elektronických komunikací* *c) Poskytování veřejně dostupné služby elektronických komunikací v pevném místě“* v nově číslovaném odst. 3 doplnit za slova *“zajištění poskytování strategicky významné služby“* slova *„podle odst. 1 a 2“.* v nově číslovaném odst. 4 doplnit za slova *„v odst. 1 a 2“* slova *„a 3“*.	událostí (přírodní katastrofy, pandemie, války atp.), které by mohly omezit možnosti využití zahraničních aktiv, ať už z důvodu faktické vzdálenosti, nebo nemožnosti uplatňovat státní moc na území jiných států. NÚKIB však prostřednictvím strategicky významných služeb spojil mechanismus zajišťování minimální úrovně dostupnosti s mechanismem prověřování bezpečnosti dodavatelského řetězce (dále jen „**BDŘ**“), přičemž se jedná o odlišné instituty jak z hlediska cíle právní úpravy, tak z hlediska způsobu jeho dosahování. Účelem stanovení minimální úrovně dostupnosti by mělo být zabezpečení dostupnosti nejkritičtějších služeb na „minimální“ úrovni potřebné k fungování společnosti a státu. Navrhovaná právní úprava se však nesoustředí na stanovení této minimální úrovně, které částečně ponechává na povinných osobách, nýbrž se věnuje konkrétním funkcím technických aktiv stanovených ve vyhlášce o nepominutelných funkcích stanoveného rozsahu. Ponechává tedy v nejistotě ohledně zabezpečení minimální úrovně dostupnosti jak poskytovatele, tak uživatele regulovaných služeb. Z výše uvedených důvodů se navrhuje oddělení mechanismu BDŘ od stanovování minimální úrovně dostupnosti. Minimální úroveň dostupnosti jednotlivých kritických služeb by měla být určena zákonem, přičemž způsob zajištění její dostupnosti by měl být ponechán na poskytovatelích. Zároveň se navrhuje konkrétní výčet služeb pro sektor telekomunikací, která respektuje přiměřenou úroveň služeb elektronických komunikací v souladu se zákonem	

		č. 127/2005 Sb., o elektronických komunikacích (dále jen „**ZEK**“). Poskytovatelé a zajišťovatelé veřejně dostupných služeb elektronických komunikací by měli mít povinnost zajistit dostupnost hlasové komunikace v mobilní síti a připojení k internetu v mobilní síti v takovém rozsahu tak, aby byla při mimořádné situaci umožněna základní komunikace mezi občany a orgány veřejné moci. Minimální úroveň by tak měla zabezpečit komunikaci během mimořádné situace, aniž by kladla nadměrné technické nároky na poskytovatele, pročež se nepočítá s nutností zajišťovat služby, které vyžadují vysokou rychlost internetového připojení, jako např. streamování videí nebo videohovory. Pokud by měla být zachována povinnost zabezpečit dostupnost regulované služby v celém rozsahu, k čemuž vede stávající podoba návrhu, museli by poskytovatelé služeb elektronických komunikací budovat infrastrukturu výlučně na území České republiky, neboť by nedávalo ekonomický smysl budovat jakoukoli infrastrukturu v zahraničí, pokud by zároveň musela existovat její plnohodnotná „záložní kopie“ v České republice. Taková povinnost by tudíž byla nepřípustným omezením volného trhu v rámci EU.	
Důvodová zpráva k Zákonu o kybernetické bezpečnosti *§ 34 Zajištění dostupnosti*	Odst. 1 vypustit V odst. 2 doplnit za slova *„cílí na rizika spojená s dostupností“* doplnit slova *„poskytované služby.“* V odst. 2 doplnit za slova *„Nicméně je limitován nutností zajistit tuto dostupnost*“ slova *„řídícím systémem*“	Znění prvního odstavce navazuje na předchozí návrh paragrafu týkajícího se lokalizace a zpracování dat, nicméně nový návrh ve znění podle § 34 je již výhradně zaměřen na zajištění dostupnosti služby z území ČR, proto je neodůvodněné se nadále zabývat tématem dostupnosti a zpracování dat.	

strategicky významné služby		Zároveň je nutné zdůraznit, že dostupnost služby a její obnova znamená realizaci takového opatření, aby v případě obnovy bylo možné takovou obnovu zajist z území České republiky a nejedná se o reálné poskytování služby z území České republiky. Předpokládáme vytvoření metodického pokynu ze strany NÚKIB, který dále upřesní plnění tohoto ustanovení.	

III. Připomínky k dalším částem zákona

Zákon o kybernetické bezpečnosti *§ 2 Vymezení pojmů*	odst. 1 písm. a) Navrhujeme doplnit za slovo „zpracování“ slova „a likvidaci“ odst. 1 písm. b) Navrhujeme za slovo „provozních“ doplnit slova „a lokalizačních“. Dále požadujeme v důvodové zprávě vymezit, o jaké procesy se jedná. odst. 1 písm. h) Navrhujeme upřesnit definici významného dodavatele.	odst. 1 písm. a) Likvidace informací a dat je jednou z klíčových oblastí správy informačních aktiv. odst. 1 písm. b) Vedle provozních údajů jsou lokalizační údaje důležitým atributem dat a informací. Navíc je zde vazba na zákon o elektronických komunikacích. Dále jasné vymezení pomůže aplikační praxi. Z textu návrhu není jasné, o jaké procesy se jedná, např. procesy vedoucí k zajištění DDI regulované služby. odst. 1 písm. h) Pokud definice upřesňuje významného dodavatele, jako toho, kdo je „významný“, dochází k jistému pojmovému zacyklení, z něhož není pro aplikační praxi návodné, o jaké dodavatele se má jednat.	

Zákon o kybernetické bezpečnosti *§ 9 Změna registrace poskytovatele regulované služby* *odst. 1*	Navrhujeme výslovně stanovit, že za změnu se považuje i výmaz, resp. ukončení regulované služby. Alternativně navrhujeme nastavení podmínek a lhůty v § 11.	Ustanovení § 9 odst. 1 nestanovuje, jak provést změnu registrace poskytovatele regulované služby směrem k podání oznámení výmazu (ukončení) regulované služby. Obecně § 9 řeší pouze registraci dalších služeb a změny režimu, avšak nezabývá se možností oznámení změn ukončení regulované služby. Navazující § 11 sice stanovuje postup výmazu z evidence poskytovatelů regulovaných služeb z pohledu NÚKIB, ale nestanovuje proces (postup) podání oznámení změn z pohledu poskytovatele, pokud již nejsou plněna příslušná kritéria. Cílem je umožnit, aby činnost, která odpadne, mohla být formálně ihned zrušena a poskytovateli nevznikaly další náklady.	
Zákon o kybernetické bezpečnosti *§13 Stanovení rozsahu řízení kybernetické bezpečnosti poskytovatelem regulované služby* *odst. 3*	Vymazat část věty *„, a odůvodnění jejich vyjmutí“*	Důvodová zpráva v prvním odstavci daného paragrafu udává, že subjekty, které již nyní postupují podle platného a účinného zákona o kybernetické bezpečnosti a vyhlášky o kybernetické bezpečnosti v procesu stanovování rozsahu řízení, budou mít situaci výrazně ulehčenou, jelikož nový postup pouze zpřesňuje již zavedenou praxi. Tuto tezi však vyvrací nová povinnost, kterou poskytovatelům ukládá právě odst. 3, § 13, který nad rámec popsaného a standardního procesu jednotlivých kroků identifikace, nastavuje povinnost naprosto opačnou, a to popsání a zdokumentování argumentace, proč daná aktiva nebyla zařazena. V krocích, které vyžaduje návrh nového zákona a prováděcí právní předpisy, však stanovuje jasně popsat i předchozí kroky, které k zařazení aktiva vedou. Pro dokumentaci a doložení argumentů, proč dané aktivum nebylo zařazeno, tedy dostačuje interpretace popisu aktiva v předchozích krocích celého procesu. Popis nad	

		rámec tohoto přináší administrativní zátěž subjektům a nepřináší přidanou hodnotu NÚKIB.	
Zákon o kybernetické bezpečnosti *§ 14 Bezpečnostní opatření* *odst. 1*	Navrhujeme vypustit druhou větu: „(1) Bezpečnostními opatřeními se rozumí úkony, jejichž cílem je zajištění řádného poskytování regulované služby a kybernetické bezpečnosti aktiv. ~~Bezpečnostními opatřeními jsou organizační a technická opatření~~.“	Dle § 14 jsou bezpečnostními opatřeními organizační a technická opatření. Vnímáme argumentaci předkladatele, že pro režim vyšších povinností jsou nastavena přísnější pravidla, zároveň není jasné, proč nelze – minimálně fakultativně – nastavit organizační a technická opatření i pro služby v režimu nižších povinností. V případě holdingu může totiž dojít k situaci, kdy některé společnosti spadnou do režimu vyšších a jiné do režimu nižších povinností. Zpravidla se však pro celý holding zpracovává jednotná řídící dokumentace a bude poměrně náročně vést dvojkolejnou dokumentaci – organizační a technická opatření pro vyšší režim a bezpečnostní opatření pro režim nižší. Ideální by bylo zachovat možnost stejného rozdělení pro oba režimy, ale věcný rozsah upravit dle typu režimu.	
Zákon o kybernetické bezpečnosti *§ 15 Seznam bezpečnostních opatření* *odst. 2 písm. c)*	Navrhujeme doplnit za slovo „řízení“ slova „aktiv a“	Řízení rizik je možné pouze tehdy, jsou-li identifikována aktiva. Teprve po identifikaci aktiv lze definovat rizika. Teze prováděcích právních předpisů k navrhované právní úpravě řízení aktiv vůbec v nižším režimu. Naopak vyhláška o bezpečnostních opatřeních poskytovatele služby v režimu vyšších povinností v § 8 výslovně stanoví řízení aktiv a v § 9 řízení rizik. Původní návrh právní úpravy, který NÚKIB předložil k veřejné konzultaci (dokument 1a str. 10 – odst. 3 písm. v) „řízení aktiv“ obsahoval. Pokud tedy nedojde k doplnění samostatného bodu týkajícího se řízení aktiv, navrhujeme spojení řízení aktiv a řízení rizik do jednoho bodu.	

Zákon o kybernetické bezpečnosti *§ 16*	Navrhujeme znění zákona přizpůsobit znění a záměru NIS2 a zachovat povinnosti pro subjekty, které odpovídají označení “essential” a “important” ve smyslu NIS2. Jiná úprava by mohla být v rozporu s NIS2 a vytvořit nerovnoměrné zatížení subjektů.	Článek 23 směrnice NIS 2 stanoví ohlašovací povinnosti základních a významných subjektů. Podle tohoto ustanovení musí základní a významné subjekty hlásit každou událost, která má významný dopad na poskytování jejich služeb. Návrh zákona implementuje článek 23 směrnice NIS 2 ve svém § 16. V porovnání se směrnicí NIS 2 stanoví § 16 pro základní subjekty přísnější pravidla než pro významné subjekty. Podle tohoto ustanovení musí významné subjekty hlásit každou událost bez ohledu na její dopad na poskytování svých služeb. NÚKIB v této souvislosti odkazuje na článek 5 směrnice NIS 2, který členským státům umožňuje přijmout nebo zachovat ustanovení zajišťující vyšší úroveň kybernetické bezpečnosti, pokud jsou tato ustanovení v souladu s právem EU. To potvrzuje i relevantní část důvodové zprávy. NÚKIB odůvodňuje tuto úpravu odkazem na stávající zákon o kybernetické bezpečnosti a uvádí, že takový přístup se v současné době uplatňuje. To nepokládáme za zcela vypovídající. Ustanovení § 8 zákona o kybernetické bezpečnosti rozlišuje oznamovací povinnosti většiny regulovaných subjektů a dále pak poskytovatelů digitálních služeb. Poskytovatelé digitálních služeb hlásí pouze takový incident, který má významný dopad na poskytování jejich služeb. Na základě výše uvedeného a s ohledem na nové rozlišení základních a významných subjektů by se na poskytovatele cloudových služeb mohla vztahovat mnohem přísnější pravidla ve srovnání se současným stavem, neboť by mohli být považováni rovněž za základní subjekty.	

		Rozšíření kompetence nad rámec stanovený NIS2 povede k i) neúměrnému vytížení subjektů a rozmělnění povinnosti oproti požadavkům dalších členských států, kde stejnou povinnost mít nebudou a zejména pak k ii) zahlcení NÚKIB reporty, které budou postrádat důležitost a výpovědní hodnotu.	
Zákon o kybernetické bezpečnosti *§ 17 Náležitosti hlášení kybernetických bezpečnostních incidentů* *odst. 3 písm. b) a c)* *odst. 5* *Vyhláška o Portálu NÚKIB a požadavcích na vybrané úkony* *§ 3 Hlášení kybernetického bezpečnostního incidentu*	Doplnit náležitosti závěrečné zprávy buď přímo do odstavce 3 nebo do § 3 Vyhlášky o Portálu NÚKIB	Paragraf 17 odst. 3 písm. b) a c) ZKB ukládá poskytovatelům regulované služby povinnost do 30 dní od oznámení incidentu nebo předložení zprávy o aktuálním stavu zvládání kybernetického bezpečnostního incidentu předložit závěrečnou zprávu, jejíž náležitosti mají být dle odst. 5 stanoveny prováděcím předpisem. Vyhláška o Portálu NÚKIB ale v § 3, který popisuje obsahové náležitosti úkonů spojených s hlášením kybernetických bezpečnostních incidentů se ale nevěnuje konkrétním náležitostem závěrečné zprávy, nýbrž pouze popisu obsahu formuláře pro hlášení incidentů, z něhož vyplývá, že slouží primárně k oznamování incidentů dle § 17 odst. 1 písm. a) nebo c) podávání průběžné zprávy o podstatných změnách stavu zvládání kybernetického bezpečnostního incidentu podle § 17 odst. 3 písm. b) zákona. Navrhujeme proto doplnit obsahové náležitosti závěrečné zprávy, aby se předešlo nejistotě regulovaných osob ohledně způsobu plnění povinností podle § 17 odst. 1 písm. b) a c), obzvláště vzhledem k tomu, že za jejich porušení hrozí dle § 58 odst. 1 písm. h) ve spojení s odst. 15 písm. a) pokuta ve výši až 250 000 000 Kč nebo do výše 2 % čistého celosvětového ročního obratu.	

Zákon o kybernetické bezpečnosti *§ 19 Informační povinnost poskytovatele regulované služby odst. 1*	V odst. 1 po slovech *„je dotčen kybernetickým bezpečnostním incidentem s významným dopadem“* doplnit slova *„, po konzultaci s poskytovatelem regulované služby,“*	V případě, že NÚKIB uloží takovou povinnost bez předchozí konzultace, může dojít k poskytnutí informací, které takový incident mohou prohloubit, případně i vyvolat další incidenty případným zveřejněním zranitelností, kterých útočník využil.	
Zákon o kybernetické bezpečnosti, *§ 19 Informační povinnost poskytovatele regulované služby odst. 2*	Na začátku odstavce 2 nahradit slova „*Poskytovatel regulované služby*“ za slova „*Dozví-li se poskytovatel regulované služby o významné kybernetické hrozbě ohrožující poskytování jím poskytované regulované služby*“.	Ze současného znění zákona není patrné, o jakých hrozbách by měl poskytovatel regulované služby uživatele informovat a zároveň je povinnost stanovena nezávisle na vědomosti poskytovatele o existenci hrozby. Povinnost je přitom spojena s nejvyšší možnou pokutou dle § 58 odst. 1 písm. k) ve spojení s odst. 15 písm. a). Navrhujeme proto jasně definovat, že poskytovatel je povinen informovat pouze o hrozbách, o kterých se dozví, a které ohrožují jím poskytovanou regulovanou službu. Dle současného znění by totiž bylo možné sankcionovat jakéhokoli poskytovatele za jakoukoli významnou hrozbu nezávisle na tom, jestli se hrozba dotýká jím poskytované regulované služby a jestli o hrozbě poskytovatel věděl nebo vědět měl.	
Zákon o kybernetické bezpečnosti *§ 19 Informační povinnost poskytovatele regulované služby odst. 2*	Ve větě první po slovech „*bez zbytečného odkladu“* doplnit slova „*informovat Úřad, který*“ a upravit slovo *„informovat“* na *„informuje“* v části věty *„způsobem informovat uživatele“*.	Informace o významné kybernetické hrozbě by měl poskytovatel regulované služby poskytnout NÚKIB, který agregovaně předá informaci širokému spektru subjektů, aby tak nedocházelo k přílišnému zahlcení pracovních kapacit poskytovatele regulované služby při nutnosti podávání individualizované informace o možnosti čelit takové hrozbě jednotlivým subjektům. Tyto kapacity pak může poskytovatel využít pro řešení	

		případné hrozby a k dalším úkonům potřebným k udržení nejvyšší úrovně kybernetické ochrany. Variantně bychom požadovali alespoň ujištění o tom, že informace předávané poskytovatelem jsou shodné s generickými informacemi podávanými subjektům čelícím významné kybernetické hrozbě.	
Zákon o kybernetické bezpečnosti *§ 23 odst. 5 a 6*	Vypustit	Navrhujeme, aby byla zrušena všechna uvedená ustanovení: § 23 odst. 5 a 6 – návrh připouští podání jen připomínek ve lhůtě 30 dnů proti vydanému opatření obecné povahy, připomínky jsou poněkud slabší nástroj ochrany ve vztahu k námitkám, o nichž je orgán vydávající opatření obecné povahy povinen samostatně rozhodnout, zrušením ustanovení se použije postup podle § 172 a násl. správního řádu, kde je možno uplatnit připomínky i námitky. Ve srovnání s připomínkami představují námitky procesně silnější nástroj ochrany práv. Dále je potřeba uvést, že jen postup podle § 172 a násl. správního řádu je zárukou uplatnění práv, povinností nebo zájmu těch, kteří jsou opatřením obecné povahy přímo dotčeni, jelikož ustanovení § 173 odst. 2 správního řádu určuje, že proti opatření obecné povahy nelze podat opravný prostředek, kterým by mohli dosáhnout nápravy. Proti opatření obecné povahy nelze podat odvolání ani rozklad (na rozdíl od správního rozhodnutí.	
Zákon o kybernetické bezpečnosti *Díl 3 Vztah*	Navrhujeme doplnit ustanovení zavazující určeného dodavatele k součinnosti při plnění zákonných požadavků poté, co byl prokazatelně informován, že se stává osobou	Dodavatel by měl mít v zákoně výslovně stanovenou povinnost spolupracovat. V praxi totiž bez součinnosti	

poskytovatele regulované služby a jeho dodavatelů	zajišťující bezpečnostně významnou dodávku strategické služby.	dodavatele nemusí být poskytovatel regulované služby schopen splnit zákonné požadavky.	
Zákon o kybernetické bezpečnosti *§ 24 Řízení dodavatelů a vztah k zadávání veřejných zakázek* *odst. 2*	Navrhujeme upřesnit v důvodové zprávě kritéria pro posouzení možnosti/nemožnosti zanesení bezpečnostních požadavků.	Jedná se o nový institut, proto by bylo vhodné koncipovat důvodovou zprávu podrobněji. Zejména jde o to, zda je poskytovatel regulované služby povinen splnit povinnosti i v případě značných nákladů.	
Zákon o kybernetické bezpečnosti *§ 25 Speciální úprava předání informací a dat od významného dodavatele* *odst. 1*	Doporučujeme navrhnout bližší specifikaci „*informace a data související s provozem aktiv soužících k poskytování regulované služby,* ***kterými významný dodavatel disponuje a které nejsou předmětem ochrany podle autorského práva***“. Doporučujeme doplnění explicitní úpravy pro situaci, kdy významný dodavatel požadovanými informacemi a daty nedisponuje, ale bude požadováno jejich opatření a následné vydání: „*Pokud významný dodavatel informacemi nebo daty souvisejícími s provozem aktiv sloužících k poskytování regulované služby nedisponuje, přesto bude účelné uložit jejich opatření a vydání, je poskytovatel regulované služby povinen uhradit významnému dodavateli v této souvislosti účelně vynaložené náklady*.“	Již v současné době působí aplikační problémy nedostatečné vymezení okruhu dat a informací spadajících pod povinnost vydání podle § 6a odst. 2 a 3 ZoKB. 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 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 za poskytovateli regulované služby, aby si vhodně ošetřil licenční	

		problematiku v soukromoprávní smlouvě. NÚKIB by neměl suplovat zanedbání těchto otázek ve smlouvě. Ve svém důsledku může takto široká 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.	
Zákon o kybernetické bezpečnosti *§ 58 přestupky* *odst. 15*	Navrhujeme v písm. a) a v písm. b) za slovo „nebo“ vložit slova „tam, kde je to vzhledem k okolnostem přiměřené“	Znění návrhu zákona věrně implementuje znění směrnice, která v souladu s judikaturou k soutěžním článkům 101 a 102 SFEU konstatuje možnost uložení pokuty za přestupek vypočítané na základě obratu podniku ve smyslu soutěžního práva, tj. ekonomické jednotky/skupiny, ke které pachatel patří. V souladu s judikaturou SDEU zdůrazňujeme „pouhou“ možnost takového postupu, tedy zabránění automatickému používání obratu skupiny jako stropu pro výpočet pokuty u pachatele, který náleží do (nějaké) skupiny/konsolidačního celku.	
Zákon o kybernetické bezpečnosti *§ 54 Vzájemná součinnost s členskými státy EU* *§ 63 Součinnost* *§ 67 Zástupce pro Českou republiku*	Působnost zákona – implementace one-stop-shop mechanismu ve smyslu článku 26 odst. 1 a 2 směrnice NIS 2 Předložený zákona o kybernetické bezpečnosti nedostatečným způsobem implementuje požadavky čl. 26 odst. 1 a 2 směrnice NIS 2. V souladu s uvedeným odůvodněním navrhujeme do § 1 návrhu zákona doplnit nové odstavce 4) a 5) s následujícím zněním: *„4) Aniž je dotčen mechanismus součinnosti podle § 60 a povinnosti k jmenování zástupce podle § 67, tento zákon se nevztahuje na osoby, které mají sídlo v jiném členském státě, s výjimkou těchto případů:*	Ačkoliv NÚKIB připomínky k nedostatečné implementaci těchto ustanovení čl. 26 odst. 1 a 2 směrnice NIS 2 v rámci veřejné konzultace odmítl, vzhledem k potenciálním negativním dopadům nesprávné implementace na této připomínce trváme. Navrhujeme proto důslednou implementaci tohoto mechanismu ve smyslu čl. 26 odst. 1 a 2 směrnice NIS 2. V rámci vypořádání připomínek NÚKIB k tomuto uvedl, že *„ustanovení § Zástupce poskytovatele regulované služby“ [resp. nyní § 67 návrhu zákona – Zástupce pro Českou republiku], resp. vymezení působnosti návrhu zákona, je třeba vnímat v kontextu § Vzájemná součinnost s členskými státy Evropské unie [resp. nyní tedy § 63 návrhu zákona – Součinnost], které ve svém*	

	a) *poskytovatel veřejně dostupné služby elektronických komunikací [poznámka pod čarou: Zákon č. 127/2005 Sb., o elektronických komunikací];* 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,* 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).*	*odst. 3 omezuje pravomoci Úřadu vůči subjektům poskytujícím služby vyjmenované v navrhovaném odst. 4 písm. c) s hlavní provozovnou mimo ČR. Úřad je vůči těmto subjektům oprávněn provést kontrolu nebo jiný úkon pouze na základě a v rozsahu žádosti o součinnost ze strany jiného členského státu, v němž má poskytovatel regulované služby umístěnu svou hlavní provozovnu.“* Citovaná ustanovení §§ 63 a 67 však implementují jen odstavce 3, 4 a 5 článku 26 směrnice NIS 2 a nijak nereflektují požadavky odst. 1 a 2, které představují tzv. one-stop-shop mechanismus, resp. tedy stanovují že některé subjekty (z povahy poskytovaných služeb) vždy budou podléhat jen jedné národní úpravě v rámci EU (nikoliv tedy jednotlivým národním úpravám v každém členském státě, kde je taková služba poskytována). Ačkoliv by bylo možné vykládat teritoriální aplikovatelnost zákona prostřednictvím přímé aplikace článku 26 směrnice NIS2, nepovažujeme takový postup za vhodnou legislativní techniku, jelikož může vyvolávat značnou právní nejistotu u adresátů tohoto zákona. Domníváme se, že vyjasnění aplikovatelnosti zákona žádným způsobem neomezuje princip součinnosti a zástupce ve smyslu §§ 63 a 67, které jsou ostatně přímo předvídány v čl. 26 odst. 3 – 5 směrnice NIS 2, a tudíž evropský zákonodárce předpokládal, že tato ustanovení budou existovat vedle sebe. Pro vyloučení pochybností o tom, že mechanismus součinnosti bude i nadále možné uplatňovat navrhujeme doplnit výslovný odkaz. Zároveň platí, že cílem návrhu zákona je implementovat směrnici NIS 2 (k tomu rovněž srov. § 1 odst. 2 návrhu zákona). Předložený návrh zákona nad rámec prosté	

	5) Pro účely tohoto zákona se má za to, že hlavní provozovna subjektu podle odst. 4 písm. b) v Evropské unii je umístěna v členském státě, v němž jsou převážně přijímána rozhodnutí týkající se opatření k řízení kybernetických bezpečnostních rizik. Nelze-li takový členský stát určit, nebo nejsou-li tato rozhodnutí přijímána v Evropské unii, má se za to, že hlavní provozovna je v členském státě, v němž daný subjekt provádí činnosti k zajištění kybernetické bezpečnosti. Nelze-li takový členský stát určit, má se za to, že dotčený subjekt má hlavní provozovnu v členském státě, v němž má provozovnu s nejvyšším počtem zaměstnanců v Evropské unii.“	implementace však obsahuje další povinnosti, které nemusí mít ve směrnici jednoznačnou oporu – např. prověřování dodavatelského řetězce ve smyslu § 28 a násl. návrhu zákona nebo požadavky na zjištění dostupnosti strategicky významných služeb ve smyslu § 34 návrhu zákona. Ačkoliv směrnice NIS 2 vychází z principu minimální harmonizace (srov. čl. 5) a veškeré povinnosti v tomto zákoně by tak měly být vykládány eurokonformně a v mezích směrnice NIS 2, při aplikaci těchto specifických povinností nemusí být zjevné, že na poskytovatele usazené v jiných členských státech EU, se tyto specifické povinnosti neuplatní, a tedy že nepodléhají působnosti českého zákona o kybernetické bezpečnosti. Jinými slovy nemusí být zjevné, že v souladu s čl. 26 odst. 1 a 2 směrnice NIS 2 podléhají jen právní úpravě členského státu, ve kterém mají hlavní provozovnu. V souladu s čl. 26 odstavce 1 a 2 směrnice NIS2 proto považujeme za klíčové vyjasnit na úrovni zákona, že český zákon o kybernetické bezpečnosti se neuplatní na vybrané subjekty, které jsou usazeny či mají hlavní provozovnu v jiném členském státě či v něm poskytují své služby, a proto podléhají právnímu řádu tohoto členského státu. 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. V souladu s čl. 26 směrnice NIS 2 se český zákon o kybernetické bezpečnosti tak uplatní pouze na:	

		- osoby sídlící v České republice, které naplní definici poskytovatele regulované služby *(standardní teritoriální princip již implementovaný v návrhu zákona)*. - poskytovatele veřejně dostupné služby elektronických komunikací, který v souladu se zákonem o elektronických komunikacích poskytuje služby na území České republiky *(čl. 26 odst. 1 písm. a) směrnice 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)*. Pro úplnost uvádíme, že obdobným způsobem byla z působnosti dosavadní směrnice „NIS1“ (směrnice (EU) 2016/1148) vyňata aplikovatelnost na poskytovatele digitálních služeb. Pro srovnání: Článek 26 odst. 1 směrnice NIS 2 Má se za to, že subjekty spadající do oblasti působnosti této směrnice **podléhají pravomoci členského státu, v němž jsou usazeny**, s výjimkou těchto případů: [….] Článek 18 odst. 1 směrnice NIS 1	

		Pro účely této směrnice se má za to, že **poskytovatel digitálních služeb podléhá pravomoci členského státu, v němž je primárně usazen**. Má-li poskytovatel digitálních služeb v některém členském státě své sídlo, má se za to, že je v tomto členském státě rovněž primárně usazen. Článek 18 odst. 1 směrnice NIS 1 byl přitom implementován ve stávajícím znění zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů, následovně: *„Tento zákon se nevztahuje na poskytovatele digitální služby, který má sídlo v jiném členském státě.“* (srov. § 33 odst. 4 zákona č. 181/2014 Sb.).	
Vyhláška o kritériích rizikovosti dodavatele Příloha bod 11	Vypustit bod 11 přílohy vyhlášky *„Je důvodná obava, že schopnost dodavatele poskytovat plnění může být významným způsobem omezena či jinak narušena*“.	Bod 11 přílohy vyhlášky nesměřuje k ochraně vůči dodavatelům, kteří představují bezpečnostní hrozbu pro Českou republiku nebo vnitřní či veřejný pořádek, ale proti dodavatelům, kteří by potenciálně nemuseli být schopni dostát svým smluvním závazkům. Čistě ekonomické schopnosti dodavatelů jsou záležitostí podnikatelského rizika poskytovatelů strategicky významných služeb, kteří pravděpodobně disponují podrobnějšími informacemi o sektoru, v němž podnikají než orgány státní správy. Jedná se tudíž o nadbytečné ustanovení, které má zbytečný potenciál omezovat svobodu podnikání poskytovatelů strategicky významných služeb. Z tohoto důvodu navrhujeme ustanovení vypustit.	
Vyhláška o regulovaných službách	Vypustit *„I. poskytovatel regulované služby v režimu vyšších povinností v případě, že sériově vyrábí osobní motorová vozidla,“*	Aktuální návrh vyhlášky stanovuje pro výrobce motorových vozidel, který vyrábí sériově osobní motorová vozidla režim vyšších povinností dle ZKB. Tím	

Příloha k vyhlášce č. [bude doplněno] Sb. *Kritéria pro identifikaci regulované služby* *7. Výrobní průmysl* *Výroba motorových vozidel (kromě motocyklů), přívěsů a návěsů*		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 směrnic do českého práva je významně se neodlišovat od ostatních členských států EU a nenarušovat tak hospodářskou soutěž v EU. Již nyní je zřejmé, že většina členských států ponechá i ve svých národních právních úpravách výrobu motorových vozidel v nižší kategorii regulovaných subjektů. S ohledem na majetkové i funkční propojení českého automobilového sektoru se zahraničím, zvláště pak Německem, je vysoce žádoucí, aby se ČR v tomto neodchylovala. V případě, že by na výrobce motorových vozidel bylo v České republice kladeno více povinností než v jiných členských státech EU, existuje nezanedbatelné riziko snížení konkurenceschopnosti českých podniků a tím narušení hospodářské soutěže. Jako nejzásadnější rozdíl mezi právní úpravou povinností subjektu ve vyšší a nižší úrovni povinností spatřujeme v povinnosti subjektu ve vyšší úrovni povinností řídit z hlediska bezpečnosti své dodavatele. Taková povinnost bude pro české výrobce motorových vozidel podstatnou zátěží. Vznikla by tak nežádoucí situace, kdy zahraniční dodavatelé nemusí být ochotni plnit zvýšené požadavky, které na ně český výrobce motorových vozidel bude muset klást. Finální výrobci by, v případě zařazení do režimu vyšších povinností, velmi pravděpodobně byli nuceni promítnout zvýšené	

		náklady do finální ceny produktu nebo přenést náklady na své dodavatele. 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 s odkazem na výše uvedené by implementace vyhlášky v navržené podobě vedla k ohrožení ekonomické činnosti těchto subjektů a přeneseně k ohrožení této podstatné části české ekonomiky. Naopak by měl český zákonodárce velmi pozorně přistupovat k tomu, aby nestanovoval nepřiměřeně přísné požadavky, a bral v potaz nastavení pravidel v dalších členských státech.	

IV. Doporučující připomínky

Zákon o kybernetické bezpečnosti *§ 45 Evidence vedené Úřadem* *odst. 1*	Navrhujeme rozšířit výčet o „dodavatele s vysokou mírou bezpečnostního rizika“	Pro zvýšení přehlednosti by bylo dobré mít k dispozici přehlednou evidenci dodavatelů s vysokou mírou rizika.	